TREBALL DE FI DE GRAU

Grau en Matemàtiques

Títol: Una aproximació a la teoria de cossos de classe

Autor: Carles Checa Nualart

Director: Óscar Rivero Salgado

Departament: Departament de Matemàtiques

Convocatòria: 2017-2018

UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

El disc 3-àdic

Una aproximació a la teoria de cossos de classe

Carles Checa Nualart
dirigit per Óscar Rivero Salgado

FME-UPC 2017/28

Índex

0 Introducció

0.1 La història de les lleis de reciprocitat

S'atribueix a Herbrand haver dit sobre la teoria de cossos de classe que cap teoria matemàtica demostrava amb unes proves tan complicades resultats tan simples i potents. Més enllà de la vanitat dels matemàtics que han aportat quelcom a aquesta teoria, crec que no erraríem si diguéssim que estem davant d'un assumpte central en l'àlgebra moderna, ja que existeixen en els cossos de classe relacions relativament senzilles amb tots els problemes que els algebristes del segle XXI segueixen estudiant: des de les corbes el·líptiques, les formes modul·lars, la seva fonamentació sobre la teoria algebraica de nombres...
L'objecte del nostre estudi seran les extensions abelianes d'un cos K. La idea de la monografia és pensar en cossos de nombres o cossos locals no arquimedians, tot i que també valdria per a altres tipus de cossos, com per exemple cossos de funcions.
Podríem començar una primera aproximació històrica a aquesta teoria per la llei de reciprocitat quadràtica.

Definició 0.1. Sigui $p \in \mathbb{Z}$ primer. Diem que a és residu quadràtic de p si l'equació $x^2 - a$ té alguna solució a $\mathbb{F}_p$[1].

Euler enuncia la llei en els següents termes. Suposem que p, q són primers senars i diferents:

1. Si algun dels primers és congruent amb 1 mòdul 4, aleshores p és residu quadràtic de q si i només si q és residu quadràtic de p.

2. Si ambdós primers són congruents amb 3 mòdul 4, aleshores p és residu quadràtic de q si i només si q no és residu quadràtic de p.

Euler es va basar en l'estudi de les formes quadràtiques representades per nombres primers, és a dir, els primers que es poden escriure de la forma $X^2 + NY^2$ per a alguna N. Més tard, amb les aportacions de Lagrange i Legendre es va millorar la notació, introduint els símbols de Legendre:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \text{ divideix } a \\ 1 & \text{si } a \text{ és residu quadràtic de } p \text{ i no és múltiple de } p \\ -1 & \text{si } a \text{ no és un residu quadràtic de } p. \end{cases}$$

Amb aquesta notació, la llei de reciprocitat quadràtica es pot escriure de la següent manera.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Gauss va donar dues proves d'aquest teorema. La primera tenia una component fortament geomètrica. La segona usava el procediment de les sumes de Gauss, és a dir, sumes de símbols de Legendre per potències d'una arrel p-èssima primitiva de la unitat i relacions entre elles. Per a efectuar càlculs amb els símbols de Legendre que ens donin resultats interessants se sol usar el criteri d'Euler, que afirma que

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Això dóna lloc a valors concrets dels símbols de Legendre, per exemple:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p = 1 \mod 4 \\ -1 & \text{si } p = 3 \mod 4. \end{cases}$$

Per demostrar el criteri d'Euler és suficient usar eines de teoria de grups sobre el grup multiplicatiu $(\mathbb{Z}/p\mathbb{Z})^\times$ i que la aplicació que a cada a l'envia al seu símbol de Legendre és un morfisme de grups.
Gauss mateix va notar que aquesta llei de reciprocitat obria les portes a la teoria moderna d'anells, ja que permetia, en un cert sentit, classificar quins elements seguirien sent primers en una certa extensió d'anells de $\mathbb{Z}$.
Per exemple, en els enters de Gauss $\mathbb{Z}[i]$, aquells primers de $\mathbb{Z}$ que es mantenien com a tals eren aquells per

[1] Gauss hagués dit, que $x^2 - a$ és divisible per p per algun x.

als quals l'equació x^2+1 no tenia cap solució, per tant els que $\left(\frac{-1}{p}\right) = -1$, o el que és el mateix (com ja hem vist), els que eren congruents amb 3 mòdul 4. Més endavant, a aquests els anomenarem primers inerts. En canvi, els que descomponen seran aquells pels quals l'equació anterior sí que té solució mòdul p, és a dir, els congruents amb 1 mòdul 4, i direm que descomponen en l'extensió $\mathbb{Z}[i]$. En aquest cas hem obviat el primer 2, en el qual sí que té solució la nostra equació, donant lloc a una descomposició en irreductibles de la forma $(1+i)(1-i)$; aquests dos elements són el mateix llevat multiplicació per unitat, i direm llavors que el primer 2 ramifica.
Aquest estudi es podrà generalitzar a altres extensions quadràtiques dels enter de la forma $\mathbb{Z}[\sqrt{d}]$ amb l'ús del símbol $\left(\frac{d}{p}\right)$. Recordem que per la llei de reciprocitat quadràtica

$$\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right),$$

i per tant si definim $p^* = (-1)^{\frac{p-1}{2}} p$ tindrem que

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right).$$

Sabem que totes les extensions quadràtiques d'un cos són de Galois amb grup de Galois $\mathbb{Z}/2\mathbb{Z} = \{\pm 1\}$. Per tant, l'aplicació $\left(\frac{p^*}{\cdot}\right)$ dóna un morfisme de grups entre el grup d'ideals primers de $\mathbb{Q}$ (relativament primers amb p) i el grup de Galois de l'extensió quadràtica $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$.
En general, el símbol de Legendre es pot generalitzar a tots els elements del cos sempre que tinguem descomposició única (DFU). Aquesta serà

$$\left(\frac{d}{N}\right) = \prod \left(\frac{d}{p_i}\right)^{n_i}$$

on $N = \prod_i p_i^{n_i}$ és la descomposició en factors primers. Aquest s'anomena símbol de Jacobi.
La utilitat del que hem explicat fins ara radica en que el símbol de Legendre codificarà informació sobre el comportament dels primers de $\mathbb{Z}$ en una extensió quadràtica de $\mathbb{Q}$, és a dir, l'aritmètica del cos base ($\mathbb{Q}$) dóna informació sobre una extensió abeliana finita, en aquest cas quadràtica ($K = \mathbb{Q}(\sqrt{p^*})$). En particular, el símbol de Legendre indica quins primers descomponen i quins són inerts en $\mathbb{Q}(\sqrt{p^*})$. És habitual referir-se a aquests resultats sobre quins primers descomponen com *l'aritmètica del cos*.
Einsenstein va generalitzar les lleis de Gauss a extensions cúbiques i biquadràtiques, afegint més congruències de primers que definien el funcionament de les extensions. Tot i així, és més il·lustrador pensar en el comportament dels primers en les extensions ciclotòmiques.
Sigui ζ_n una arrel n-èssima primitiva de la unitat. En aquesta extensió podem construir el següent símbol, definit per a primers p tals que $(p,n) = 1$:

$$\left(\frac{p}{\mathbb{Q}(\zeta_n)/\mathbb{Q}}\right) = \rho,$$

amb $\rho = \zeta_n^p$, i que es pot entendre com un element del grup de Galois (ja que sabem és isomorf a $(\mathbb{Z}/m\mathbb{Z})^\times$, o alternativament al grup d'arrels de la unitat primitives mòdul n). En aquestes extensions direm que un primer ramifica si divideix al nombre n. Tindrem una classe especial de primers distingits, aquells que via aquesta aplicació van al neutre: seran els primers del tipus $kn+1$ i són els que descomponent completament en l'extensió ciclotòmica. Per a veure la relació de la teoria de cossos de classe amb aquestes lleis de reciprocitat, a la secció d'aplicacions posarem aquests símbols amb tot el detall per a un cos de nombres qualsevol i veurem com les lleis de reciprocitat es desprenen fàcilment dels resultats ja demostrats.
Dirichlet va treballar en els resultats sobre els cossos ciclotòmics i va intentar extreure'n conclusions respecte a la quantitat de primers existent en un cos de nombres determinat i va introduir els anomenats caràcters de Dirichlet, que defineixen morfismes de grups χ entre les unitats de $\mathbb{Z}/m\mathbb{Z}$ i $\mathbb{C}^\times$. Observi's que a la imatge només tenim arrels de la unitat. A aquests caràcters li podem associar unes sèries concretes que anomenem L-sèries:

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1-\chi(p)p^{-s})^{-1}$$

La introducció d'aquestes sèries per part de Dirichlet i Riemann denota una manera fortament analítica de pensar la teoria de cossos de classe i demostrar-ne els resultats, que no seguirem durant el transcurs del treball. Però, com bé apuntava Herbrand, ens permet obtenir resultats força senzills com, per exemple, el teorema de la progressió aritmètica de Dirichlet.

Teorema 0.1. Siguin a, m enters sense divisors en comú. Existeixen infinits nombres primers de la forma $p = a + mn$ per $n \in \mathbb{Z}$.

Aquest teorema pot ser extrapolat a nocions més amplies a l'hora de comptar primers en una extensió, com és el teorema de Chebotarev, que en particular ens dirà que el conjunt de primers del teorema anterior té densitat de Dirichlet $\frac{1}{\varphi(m)}$, entenent la densitat d'un conjunt de primers $S \subset \mathbb{P}$ (on $\mathbb{P}$ denota el conjunt de tots els primers de $\mathbb{Z}$) com:

$$\delta(\mathbb{P}) = \lim_{n\to\infty} \frac{|\{p \in S \text{ tal que } p \leq n\}|}{|\{p \in \mathbb{P} \text{ tal que } p \leq n\}|}.$$

El primer compendi generalitzat de totes les lleis de reciprocitat i aproximació als resultats de la teoria de cossos de classe tal i com els presentarem va ser donat per Hilbert en el seu llibre *Zahlbericht*, l'any 1897, tot i que molts dels resultats no van ser desenvolupats tal i com els presentarem fins als anys 30 per matemàtics com Artin, Hasse, Hecke, Weil o Takagi.
En aquest llibre es troba la primera prova correcta del teorema de Kroenecker-Weber, que afirma que qualsevol extensió abeliana de $\mathbb{Q}$ està continguda en una extensió ciclotòmica. Els dos matemàtics que donen nom al teorema havien ja proporcionat proves aproximades, però amb errors en alguns casos particulars com en les extensions de discriminant potència de 2.
El llibre també conté el que avui coneixem com teorema 90 de Hilbert i un apèndix sobre teoria de Kummer per a un tipus particular de cossos, a més d'un resum de les lleis de reciprocitat introduint els símbols de Hilbert, que són generalitzacions dels símbols anteriors per a un tipus concret de formes quadràtiques que deixen entreveure la necessitat d'obtenir primer resultats per a cossos locals, com per exemple $\mathbb{Q}_p$ (aquests resultats estaven sent desenvolupats simultàniament per Hensel i Kummer).

Definició 0.2. Sigui p un nombre primer. Un enter p-àdic a $\mathbb{Z}_p$ és una sèrie de la forma $\sum_{n=0}^{\infty} a_n p^n$ amb $a_n \in \mathbb{Z}/p\mathbb{Z}$. $\mathbb{Z}_p$ és un anell íntegre amb les operacions suma i producte naturals.

Prendrem $\mathbb{Q}_p$ com el cos de fraccions d'aquest anell. En el capítol 2 veurem que aquests cossos són la compleció de $\mathbb{Q}$ respecte una certa valoració. L'avantatge d'aquests cossos és que només tindran un ideal maximal, que serà el generat per p ($\mathbb{Z}_p$ és un anell de valoració discreta), i això facilitarà de forma notable l'estudi de qüestions aritmètiques.

0.2 El programa de la teoria de cossos de classe

Un cop fet aquest petit repàs històric, podem dir que els objectius de la teoria de cossos de classe són principalment els següents.

1. Descriure totes les extensions abelianes d'un cos de nombres K només en termes de l'aritmètica de K. Per això hem de relacionar el que abans hem definit com *aritmètica del cos* amb la construcció del grup de classes, un cert grup construït a partir dels ideals de l'anell d'enters de K (sovint direm directament els ideals de K, tot i que només hi ha dos ideals en el cos).

2. Descriure el grup de Galois de les extensions abelianes del cos en termes d'aquesta aritmètica.

3. Descriure la descomposició dels ideals primers en aquestes extensions abelianes.

Per a qualsevol extensió abeliana L/K es defineix el símbol d'Artin com l'aplicació

$$\left(\frac{\cdot}{L/K}\right) \quad \{\text{Ideals primers de } K\} \to \text{Gal}(L/K),$$

de manera que quan dotem d'estructura de grup als ideals esdevé un morfisme de grups (observem que per a definir aquesta aplicació s'han d'excloure els primers que ramifiquen en l'extensió). A més, factoritzant a través d'un cert subgrup *nucli* esdevé un isomorfisme. Aquest nucli serà, bàsicament, el subgrup $\text{Nm}(L)$ on

L és la pròpia extensió, és a dir, les normes de tots els elements de l'extensió (un cop excloem la ramificació) dins el grup d'ideals. Per això, a les extensions L les anomenarem cossos de classe. Amb això també podrem construir extensions L/K que compleixin les propietats que a nosaltres ens interessin en termes dels ideals primers, és a dir, en el que definirem com ramificació. A més, cada ideal primer tindrà imatge en un element concret del grup de Galois que anomenarem Frobenius. Alguns resultats dels quals es va tardar força anys en trobar una demostració seran simples corol·laris d'aquesta llei de reciprocitat, com el Kroenecker-Weber. També veurem que en el camí cap a la demostració també podem trobar-ne d'altres.
Per suposat, aquest programa serà més fàcil quan en el cos K només tinguem un ideal primer, donant lloc a la teoria local de cossos de classe. A més en aquest cas podrem agafar com a grup de classe el propi grup multiplicatiu del cos.
També haurem de veure perquè tots aquests resultats només valen per a extensions abelianes. Això es deu a què si prenem l'extensió abeliana maximal continguda en una extensió donada, els subgrups de norma seran els mateixos. Per aprofundir més en aquest problema, Robert Langlands, premi Abel d'aquest any, va proposar l'intent de relacionar els grups de classe amb representacions de Galois (endomorfismes d'espais vectorials dotats de la mateixa estructura que un grup de Galois) de les extensions no abelianes. La majoria de les conjectures proposades per ell encara es troben sense demostració.
L'estructura del treball serà la següent.

1. En el capítol inicial, presentarem una sèrie de resultats aritmètics sobre teoria algebraica de nombres necessaris per entendre els resultats centrals del treball, així com la demostració donada per Hilbert del teorema de Kroenecker-Weber.

2. En el segon, presentarem els cossos locals i les seves extensions, fent visible perquè resulta més senzill demostrar certs resultats en aquest context.

3. En el tercer, desenvoluparem l'eina bàsica per demostrar aquests resultats de manera moderna, que és la cohomologia de grups. Aquesta teoria serveix com a mètode general per a moltes altres branques de la teoria de nombres com les corbes el·líptiques o la teoria de formes modulars, al mateix temps que ja sabem que és una de les eines fonamentals en la topologia algebraica. Aquesta secció acabarà amb l'enunciat del teorema de Tate, que relaciona grups de cohomologia de la mateixa paritat, i per tant, quan els relacionem amb els nostres objectes, valdrà com a morfisme per derivar la llei de reciprocitat d'Artin.

4. El quart capítol donarà tots els resultats necessaris de la teoria local, demostrant primer la llei de reciprocitat i veient que compleix el que nosaltres imposem per al morfisme de Frobenius. També construirem tots els subgrups de norma per a qualsevol cos local.

5. En el cinquè capítol, enunciarem tots els resultats de la teoria en el cas global. Per fer això, necessitarem treballar amb un cos global que entenem com a producte infinit de cossos locals, i apareixeran alguns problemes topològics relacionats amb la compacitat local. Amb la finalitat de solucionar aquests problemes, introduirem la notació adèlica (uns nous anells que anomenarem adèles), que és la més utilitzada per descriure la reciprocitat d'Artin sense ús d'eines analítiques. Amb això, tornarem a usar els resultats de cohomologia amb els idèles i recuperarem els mateixos resultats en aquest context.

6. A la secció final, a mode de conclusió, parlarem de quines aplicacions té la teoria de cossos de classe global, intentant abraçar resultats que es desprenguin de manera relativament senzilla, com per exemple les lleis de reciprocitat presentades en aquesta secció a mode de motivació. Tot i així, donada la centralitat del que haurem demostrat, les conseqüències s'escaparan fàcilment de les nostres mans.

1 Preliminars de teoria algebraica de nombres

1.1 Ideals fraccionaris i grup de classes

Definició 1.1. Un anell de Dedekind és un anell A que compleix les tres següents propietats.

1. A és Noetherià, és a dir, tot ideal és finitament generat.
2. A és integralment tancat, és a dir, és la clausura entera del seu cos de fraccions.
3. Tot ideal primer diferent del zero és maximal.

El següent resultat és el més rellevant sobre aquest tipus d'anells.

Teorema 1.1. En un anell de Dedekind, tot ideal $\mathfrak{a}$ descomposa de manera única com a producte d'ideals primers de la forma $\mathfrak{a} = \mathfrak{p}_1^{n_1} \dots \mathfrak{p}_s^{n_s}$.

Recordem que un mòdul sobre l'anell A és un grup M on fem actuar l'anell. Un submòdul és un subgrup de M on al fer actuar A ens mantenim dins del subgrup. Un ideal de l'anell A, per exemple, és un mòdul sobre A, i de fet, es pot veure també com un submòdul d'A.
Així, si el nostre objectiu és estudiar la aritmètica d'un cos (o del seu anell d'enters), ens interessa poder definir una operació sobre els ideals no nuls que ens doni una operació de grup.

Definició 1.2. Sigui K un cos i A el seu anell d'enters. Un ideal fraccionari $\mathfrak{a}$ és un A-submòdul de K tal que existeix $d \in A$ tal que $d\mathfrak{a} \subset A$.

Exemple 1.1. Els ideals d'A són ideals fraccionaris. Els submòduls del tipus $(\frac{c}{d})$ (amb $d \neq 0$) són un altre exemple.

Donat que A és noetherià, tots els ideals fraccionaris són finitament generats. Si estan generats per un sol element els direm principals. Definim el producte d'ideals fraccionaris igual que el d'ideals en un anell qualsevol

$$\mathfrak{ab} = \Big\{ \sum_i a_i b_i \,|\, a_i \in \mathfrak{a}\ b_i \in \mathfrak{b} \Big\}.$$

De manera senzilla es veu que aquest producte és associatiu i commutatiu. L'ideal total K actua com a element neutre. Per últim, resta comprovar que tot ideal fraccionari té un invers.

Lema 1.1. Sigui $\mathfrak{a} \subset K$ un ideal fraccionari. Definim

$$\mathfrak{a}' = \big\{ a \in K \,|\, a\mathfrak{a} \subset A \big\}.$$

Llavors, $\mathfrak{a}'$ és un ideal fraccionari i satisfà $\mathfrak{a}\mathfrak{a}' = A$.

Demostració. Per la pròpia definició, tenim $\mathfrak{a}\mathfrak{a}' \subset A$ i clarament és un ideal. En cas que no sigui el total, estarà contingut en un ideal primer $\mathfrak{p}$ [2]. Sigui $A_\mathfrak{p}$ la localització en aquest ideal, i siguin $\mathfrak{b}, \mathfrak{b}', \mathfrak{q}$ les imatges de $\mathfrak{a}, \mathfrak{a}', \mathfrak{p}$; es satisfà $\mathfrak{b}\mathfrak{b}' \subset \mathfrak{q}$. Observem que $\mathfrak{q}$ és l'únic ideal primer i estarà generat per un uniformitzador π. Per altra banda, $\mathfrak{b}$ també serà principal generat per algun π^m i per la pròpia definició, $\mathfrak{b}'$ estarà generat pel seu invers π^{-m}, la qual cosa implica que $\mathfrak{b}\mathfrak{b}' = A_\mathfrak{p}$, que contradiu la inclusió dins $\mathfrak{q}$. □

En particular per als ideals fraccionaris principals no nuls (d) el seu invers és (d^{-1}).
Amb això ja tenim que els ideals fraccionaris formen un grup I_K, del qual els principals P_K en formaran un subgrup.

Definició 1.3. El grup de classes d'un cos K és el grup quocient dels ideals fraccionaris per els ideals fraccionaris principals

$$C_K = \frac{\text{Ideals fraccionaris}}{\text{Ideals fraccionaris principals}} = I_K / P_K.$$

[2] En els anells de Dedekind, els primers no zero i els maximals són els mateixos. A més, qualsevol ideal no trivial està contingut en un maximal.

Anomenem nombre de classes a l'ordre d'aquest grup. Un dels teoremes més rellevants de la teoria algebraica de nombres clàssica és que per a qualsevol cos K el nombre de classes és finit. Aquest teorema es basa en trobar una fita per al nombre de classes depenent del grau d'aquest cos de nombres sobre $\mathbb{Q}$ i el nombre d'immersions d'aquest cos en els complexos. Aquesta s'anomena la fita de Minkowski i el seu valor és

$$\sqrt{|D|}\Big(\frac{4}{\pi}\Big)^{r_2}\frac{n!}{n^n},$$

on r_2 és el nombre de parells d'immersions complexes conjugades, D és el discriminant de l'extensió i n és el grau. *Milne, ANT, 4*

1.2 Extensions d'ideals primers

L'esquema que estarem seguint quan parlem de primers en un cos serà el següent. Prenem K un cos i L una extensió algebraica finita. Siguin $\mathcal{O}_K$ i $\mathcal{O}_L$ els anells d'enters de cadascun dels cossos (que suposem que són de Dedekind). En particular, ambdós són anells íntegrament tancats i $\mathcal{O}_L$ és la clausura entera de L en $\mathcal{O}_K$. Per tant, tenim el següent esquema:

$$\begin{array}{ccc} \mathcal{O}_L & \longrightarrow & L \\ \uparrow & & \uparrow \\ \mathcal{O}_K & \longrightarrow & K \end{array}.$$

Sigui $\mathfrak{p}$ un ideal primer a $\mathcal{O}_K$. Aleshores, l'ideal estès sota la inclusió $\mathfrak{p}\mathcal{O}_L$ no té perquè seguir sent un ideal primer[3]. Però com que és un ideal en un anell de Dedekind, sí que tindrà alguna descomposició en els primers de l'anell de la forma

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\dots\mathfrak{P}_g^{e_g}.$$

En particular sabem que els primers $\mathfrak{p}$ i $\mathfrak{P}_i$ donaran lloc al que anomenarem cossos residuals (al fer quocient per ells), que anomenarem $k = \mathcal{O}_K/\mathfrak{p}$ i $l_i = \mathcal{O}_L/\mathfrak{P}_i$. Es comprova fàcilment que $k \subset l_i$. En particular, aquesta serà una extensió finita de cossos finits. Definim f_i com el grau d'aquesta extensió.

Teorema 1.2. Sigui L/K una extensió algebraica finita de grau n i $\mathfrak{p}$ un primer amb una descomposició com la descrita anteriorment. Aleshores, $\sum_{i=1}^{g} e_i f_i = n$. En particular si l'extensió és de Galois, tots els e_i i tots els f_i són iguals i per tant l'equació anterior s'escriu com $efg = n$.

Hi ha alguns casos del resultat anterior que tindran un interes especial.

Definició 1.4. Amb les notacions anteriors, sigui L/K una extensió de Galois. Llavors, segons el comportament dels coeficients e, f, g:

1. si $e = f = 1$, diem que $\mathfrak{p}$ descompon completament;
2. si $g = f = 1$, diem que $\mathfrak{p}$ ramifica completament;
3. si $e = g = 1$, diem que $\mathfrak{p}$ és inert.

Podem també classificar quins seran els primers que ramificaran, és a dir, aquells que tenen $e > 1$.

Teorema 1.3. Suposem que $\mathcal{O}_L$ és lliure com a $\mathcal{O}_K$-mòdul, és a dir, té una base. Aleshores, un primer $\mathfrak{p} \subset \mathcal{O}_K$ ramifica, si i només si, divideix el discriminant de l'extensió.

1.3 L'element de Frobenius

La següent definició serà clau durant tot el treball. Recordem que en les extensions de cossos finits existeix un element privilegiat que genera el seu grup de Galois.

Definició 1.5. Sigui $\mathbb{F}_q$ un cos de característica p. L'endomorfisme de Frobenius es defineix com la aplicació

$$\mathrm{Frob}_q(x) = x^q.$$

[3]Un exemple molt fàcil de que la imatge d'un ideal primer per un morfisme d'anells no és necessàriament un ideal primer es basa en considerar la inclusió $\mathbb{Z} \hookrightarrow \mathbb{Q}$; llavors $p\mathbb{Z}$ dóna a $\mathbb{Q}$ l'ideal total.

Definim com a cos perfecte de característica p aquell on aquest endomorfisme és bijectiu.
En el cas dels cossos finits l'endomorfisme de Frobenius és bijectiu. A més, es pot veure que una extensió de grau d de $\mathbb{F}_p$ tindrà grup de Galois cíclic generat per aquest element de Frobenius amb $q = p^d$.
Volem generalitzar aquesta noció als cossos amb els que treballarem, que són extensions de $\mathbb{Q}$ i de $\mathbb{Q}_p$. Per fer-ho, podem usar el fet de que els cossos residuals sí que tenen característica finita. Donat $\sigma \in \mathrm{Gal}(L/K)$, és natural preguntar-se si és possible considerar aquest mateix endomorfisme a nivell de cossos residuals, és a dir, si existeix $\hat{\sigma}$ de manera que

$$\hat{\sigma} : \mathcal{O}_L/\mathfrak{P} \to \mathcal{O}_L/\mathfrak{P}, \qquad \hat{\sigma}[x] = [\sigma(x)]$$

estigui ben definida. Per això, s'ha de requerir que $\sigma(\mathfrak{P}) = \mathfrak{P}$.

Definició 1.6. El grup de descomposició d'un primer $\mathfrak{P}$ a $\mathcal{O}_L$, que denotem $D_{\mathfrak{P}}$, és

$$D_{\mathfrak{P}} := \{\, \sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Teorema 1.4. Amb les notacions de la secció anterior, el grup de descomposició $D_{\mathfrak{P}}$ té ordre ef.

Demostració. Podem definir una acció de Galois sobre els ideals primers de L que es troben per sobre d'un primer $\mathfrak{p}$ de $\mathcal{O}_K$ fixat; això és així ja que $\sigma(\mathfrak{P})$ és també un ideal maximal de L per sobre de $\mathfrak{p}$. Es comprova fàcilment que aquesta acció és transitiva. Per tant, per la fòrmula de les òrbites, l'ordre del grup descomposició és el grau de l'extensió entre el nombre de maximals que tenim per sobre, és a dir, $\frac{n}{g} = ef$. □

Definició 1.7. Usant les notacions de l'apartat anterior, sigui $\tau \in \mathrm{Gal}(L/K)$ complint les següents condicions:

1. $\tau \in D_{\mathfrak{P}}$.
2. Per tot $x \in \mathcal{O}_L$, ${}^{\tau}x = x^q \mod \mathfrak{P}$, on q és el nombre d'elements del cos residual $\mathcal{O}_K/\mathfrak{p}$.

Direm que τ és un element de Frobenius. Notarem aquests elements com $(\mathfrak{P}, L/K)$ o $\mathrm{Frob}_{L/K}$.

Definirem la norma de l'ideal primer $\mathfrak{p}$ de $\mathcal{O}_K$ com $N(\mathfrak{p}) = q$, essent q la cardinalitat del cos residual.
Podem definir de manera natural un morfisme del grup de descomposició al grup de Galois de l'extensió de cossos residuals,

$$\varphi : D_{\mathfrak{P}} \to \mathrm{Gal}(l/k).$$

Aquesta aplicació serà exhaustiva ja que tot element de $\mathrm{Gal}(l/k)$ fixarà l'ideal $\mathfrak{P}$. També podem veure que el Frobenius que hem definit està a l'antiimatge del Frobenius de $\mathrm{Gal}(l/k)$. Per tenir un isomorfisme hem de factoritzar pel nucli, i llavors definim el grup d'inèrcia de la següent manera.

Definició 1.8. Amb les notacions anteriors, el grup d'inèrcia associat al primer $\mathfrak{P}$ de $\mathcal{O}_L$ és

$$I_{\mathfrak{P}} = \{\, \sigma \in \mathrm{Gal}(L/K) \,|\, \sigma(\alpha) = \alpha \mod \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L\}.$$

Si demostrem que $I_{\mathfrak{P}}$ és el nucli de l'aplicació φ anterior, haurem demostrat que $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(l/k)$. També haurem vist que l'ordre de $I_{\mathfrak{P}}$ és e.

Proposició 1.1. $I_{\mathfrak{P}}$ és el nucli de l'aplicació φ.

Demostració. Prenem $\overline{x} \in l$ i li apliquem un element de $I_{\mathfrak{P}}$. Prenem un representant seu $x \in \mathcal{O}_L$ i sabem que es mou a un altre element de la mateixa classe. Per tant, $\overline{x}$ queda fix per $I_{\mathfrak{P}}$. Recíprocament, qualsevol element que estigui al nucli satisfà les condicions de la inèrica. □

Corol·lari 1.1. Un primer descompon completament, si i només si, el grup de descomposició és trivial.

Això es demostra només mirant els ordres dels grups.

Lema 1.2. En el cas que $\mathfrak{p}$ no ramifiqui, donat un primer $\mathfrak{P}$ a $\mathcal{O}_L$ existeix un únic element de Frobenius.

Finalment, ens falta demostrar que podem definir $\left(\frac{\mathfrak{p}}{L/K}\right)$ independentment de quin sigui el primer $\mathfrak{P}$ triat en la seva descomposició (llevat de conjugació). Per això, ens cal el següent teorema que ens dona moltíssima més informació de la que necessitem. Usarem una part d'aquesta informació en el capítol 6, quan parlem de la teoria de cossos de classe global.

Proposició 1.2. Sigui L/K una extensió de Galois i $\mathfrak{p}$ un primer de K que no ramifiqui. Donat $\mathfrak{P}$ un primer de L per sobre de $\mathfrak{p}$, es donen les següents tres propietats.

1. Si $\sigma \in \mathrm{Gal}(L/K)$, aleshores
$$\left(\frac{\sigma(\mathfrak{P})}{L/K}\right) = \sigma \left(\frac{\mathfrak{P}}{L/K}\right) \sigma^{-1}.$$
2. L'ordre de $\left(\frac{\mathfrak{P}}{L/K}\right)$ és f.
3. $\mathfrak{p}$ descompon completament, si i només si, $\left(\frac{\mathfrak{P}}{L/K}\right) = 1$.

Demostració. Fent ús de l'unicitat del morfisme de Frobenius en el cas no ramificat, prenem $a \in L$, i per simplificar la notació escriurem $\tau' = \left(\frac{\sigma(\mathfrak{P})}{L/K}\right)$ i $\tau = \left(\frac{\mathfrak{P}}{L/K}\right)$. Aleshores

$$\tau'(a) - a^q \in \sigma(\mathfrak{P}') \iff \sigma^{-1}\tau'(a) - \sigma^{-1}(a^q) \in \mathfrak{P} \iff \sigma^{-1}\tau'\sigma(\sigma^{-1}a) - \sigma^{-1}(a^q) \in \mathfrak{P} \iff \sigma^{-1}\tau'\sigma = \tau.$$

Així, com que $\mathfrak{p}$ no ramifica, tenim $D_{\mathfrak{P}} = \mathrm{Gal}(l/k)$, per tant el nostre element és un element generador d'aquests grups que tenen ordre f. En el cas que descomponguin completament, també tenim $f = 1$. □

Amb aquest resultat podem veure que, en una extensió abeliana L/K, donats $\mathfrak{P}, \mathfrak{P}'$ dos primers per sobre de $\mathfrak{p}$, existeix un σ, tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Aleshores,

$$\left(\frac{\mathfrak{P}'}{L/K}\right) = \left(\frac{\sigma(\mathfrak{P})}{L/K}\right) = \sigma \left(\frac{\mathfrak{P}}{L/K}\right) \sigma^{-1} = \left(\frac{\mathfrak{P}}{L/K}\right).$$

Per tant, en el cas abelià podem definir $\left(\frac{\mathfrak{p}}{L/K}\right)$ com qualsevol d'aquests elements.

1.4 El teorema de Kronecker-Weber

Teorema 1.5. (*Kroenecker-Weber*) Tota extensió abeliana $K/\mathbb{Q}$ està continguda en una extensió ciclotòmica.

La rellevància d'aquest teorema radica en que és la primera classificació possible d'una extensió abeliana. Per això, hauríem de trobar quina és l'extensió ciclotòmica minimal en la que està continguda.

Exemple 1.2. Si prenem l'extensió $\mathbb{Q}(\sqrt{5})$ sobre $\mathbb{Q}$ estarà continguda en l'extensió ciclotòmica $\mathbb{Q}(e^{\frac{2\pi i}{5}})$ ja que $\sqrt{5} = e^{\frac{2\pi i}{5}} - e^{\frac{4\pi i}{5}} - e^{\frac{6\pi i}{5}} + e^{\frac{8\pi i}{5}}$.

La primera demostració acceptada és de Hilbert, que va corregir els errors que els dos matemàtics mencionats van cometre en alguns dels primers que preteniem ramificar.
Ens interessa principalment entendre les eines que s'usen ja que algunes apareixeran més endavant.

Teorema 1.6. (*Minkowski*) Qualsevol extensió finita de $\mathbb{Q}$ té discriminant $\Delta \neq \pm 1$. Per tant, ramificarà en algun primer p.

Definició 1.9. Sigui L/K una extensió de cossos de nombres i $\mathcal{O}_K, \mathcal{O}_L$ els anells d'enters respectius. Prendrem un primer $\mathfrak{p} \subset \mathcal{O}_K$ i un altre $\mathfrak{P} \subset \mathcal{O}_L$ que estigui en la descomposició de $\mathfrak{p}\mathcal{O}_L$. Direm que $\mathfrak{P}$ és mansament ramificat en l'extensió si l'índex de ramificació e és relativament primer amb la característica del cos residual $\mathcal{O}_K/\mathfrak{p}$. Altrament direm que és salvatgement ramificat.

Definició 1.10. Els subgrups d'inèrcia superiors es defineix com la seqüència donada per

$$E_n = \{\, \sigma \in \mathrm{Gal}(L/K) \mid \overline{\sigma(x)} = \overline{x} \mod \mathfrak{P}^{n+1} \ \forall x \in \mathcal{O}_L \,\}.$$

En particular, per $n = 0$ obtenim el grup d'inèrcia $I_{\mathfrak{P}}$ (i a més entendrem que per $n = -1$, la definició equival al grup de descomposició $D_{\mathfrak{P}}$).

Òbviament tots són subgrups del grup d'inèrcia i són normals en el immediatament posterior, i per tant donen lloc a la successió de subgrups

$$\ldots E_2 \trianglelefteq E_1 \trianglelefteq I_{\mathfrak{P}} \trianglelefteq D_{\mathfrak{P}}.$$

Si comprovem que els quocients són abelians, haurem demostrat que el grup de descomposició és resoluble.

Corol·lari 1.2. $\mathfrak{P}$ és mansament ramificat en l'extensió si, i només si, els grups de ramificació d'ordre superior (a partir de $n \geq 1$) són trivials.

Fet això, ens podem dotar d'eines per veure que n'hi ha prou amb demostrar el teorema de Kronecker-Weber per al cas de ramificació salvatge.

Proposició 1.3. Sigui $p \in \mathbb{Z}$ primer i $K/\mathbb{Q}$ una extensió abeliana mansament ramificada. Existeixen una altra extensió $K'/\mathbb{Q}$ i un subcos $L \subset \mathbb{Q}(\zeta_n)$ per alguna arrel n-èssima de la unitat tal que:

1. Qualsevol primer que no ramifiqui a K, tampoc ho fa a K'.
2. El primer p no ramifica a K'.
3. Es compleix: $LK = LK'$.

Demostració. Fixem un primer $\mathfrak{P}$ de K dividint p. pel corol·lari anterior, sabem que E_1 és trivial, i amb això es pot demostrar que el subgrup d'inèrcia $I_{\mathfrak{P}}$ es pot injectar dins $\mathbb{F}_p^\times$. Això implica que e (l'índex de ramificació) divideix $p-1$.
Podem prendre una subextensió $L \subset \mathbb{Q}(\zeta_p)$. En aquest cas, p seguirà sent totalment ramificat i alhora mansament ramificat. Prendrem $\mathfrak{Q}$ com l'únic primer de L que quedi per sobre de p.
Ara podem considerar la composició KL i $\mathfrak{U}$ un primer que quedi per sobre de $\mathfrak{Q}$. Podem prendre K', el subcos de KL fix per la inèrcia $I_{\mathfrak{U}}$. Ara només ens cal demostrar les tres propietats per a aquests cossos.
Per a la propietat 1, prenem un primer $q \in \mathbb{Z}$ que no ramifiqui a K. Aleshores q no divideix el discriminant de K ni tampoc divideix el discriminant de L ja que p és l'únic que ramifica i $q \neq p$. Per tant, tampoc dividirà el discriminant de KL i com a tal tampoc el de K'.
Per a la propietat 2, és senzill veure que cap primer ramifica en el cos fix del seu propi grup d'inèrcia. De fet, en el següent capítol veurem que això caracteritza les extensions no ramificades.
Ens falta demostrar la propietat 3. Sabem que a l'extensió L només ramifica el primer p, per tant ha de tenir grau $[L:\mathbb{Q}] = p^m$ que també equival és igual al grau $[KL:K']$. Tal i com hem construït l'extensió, també sabem que $K'L \subset KL$. Prenent graus,

$$[K'L:\mathbb{Q}] = [K':\mathbb{Q}] \cdot [L:\mathbb{Q}] = [KL:K'] \cdot [K':\mathbb{Q}] = [KL:\mathbb{Q}],$$

on a la primera igualtat hem fet servir que $K' \cap L = \mathbb{Q}$ ja que cap primer ramifica en ambdós simultàniament, i si no fos trivial, es contradiria el teorema de Minkowski. □

Proposició 1.4. N'hi ha prou amb demostrar el teorema per al cas en què $[K:\mathbb{Q}] = p^k$ per a algun primer $p \in \mathbb{Z}$, $\mathrm{Gal}(K/\mathbb{Q})$ és cíclic, i p és l'únic primer que ramifica.

Demostració. La proposició anterior ens permet veure que podem suposar que p és l'únic primer que ramifica. També podem suposar que és cíclica ja que qualsevol extensió abeliana és composició de extensions cícliques. □

Ara ens reduirem a un cas més senzill encara, que és aquell en que l'extensió és de grau p i el discriminant una potència de p. Coneixem els dos resultats següents:

Proposició 1.5. Donat un primer senar, existeix una única extensió $K/\mathbb{Q}$ d'ordre p amb discriminant potència de p. En particular, aquesta és l'única subextensió de grau p de $\mathbb{Q}(\zeta)$ on ζ és una arrel p^2-èssima de la unitat.

Demostració. Al prendre la subextensió $K \subset \mathbb{Q}(\zeta_{p^2})$ de grau p només p ramificarà, i per tant el discriminant és una potència de p. En particular, el discriminant és $(-1)^{\frac{p-1}{2}} p^{p-2}$; aquí s'ha de fer servir que p és imparell. Això ens demostra l'existència de tal cos.
Prenem K' una altra extensió amb les mateixes propietats i anem a veure que $K = K'$. Si demostrem que una extensió on p sigui l'únic primer que ramifiqui ha de ser cíclica, aleshores $\mathrm{Gal}(KK'/\mathbb{Q})$ ha de ser cíclica, però si les dues extensions no són iguals, aquesta extensió té grau major a p. El grup de Galois serà un subgrup de $\mathrm{Gal}(K'/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$, que no té cap element d'ordre major a p, el qual contradiu que l'extensió KK' sigui cíclica. □

Lema 1.3. Sigui $K/\mathbb{Q}$ una extensió de grau p on l'únic primer que ramifica és p. Aleshores $K/\mathbb{Q}$ és una extensió cíclica.

Ometrem la demostració d'aquest lema de cara a la senzillesa expositiva. Com és habitual en la teoria de nombres s'ha de tractar el cas $p = 2$ de manera independent, ja que hi solen passar fenòmens diferents.

Proposició 1.6. Les úniques extensions quadràtiques amb discriminant una potència de 2 són: $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ i $\mathbb{Q}(i)$

Demostració. Sabem que els discriminants de les extensions quadràtiques $\mathbb{Q}(\sqrt{d})$ són d si $d \equiv 1 \bmod 4$, i $4d$ si $d \equiv 2, 3 \bmod 4$. Per tant, només poden ser aquest tres casos. □

El que volen il·lustrar aquests teoremes és que, donat un primer p, l'estratègia de demostració es basa en afegir arrels p^n-èssimes de la unitat.

$$\begin{array}{c} \mathbb{Q}(\zeta_{p^n}) \\ \cdots \\ | \\ \mathbb{Q}(\zeta_{p^2}) \\ | \\ \mathbb{Q}(\zeta_p) \\ | \\ \mathbb{Q} \end{array}$$

Podem encarar ara el resultat definitiu que ens demostra Kroenecker-Weber.

Proposició 1.7. Qualsevol extensió cíclica $K/\mathbb{Q}$ de grau p^n amb discriminant potència de p està continguda a dins de $\mathbb{Q}(\zeta_{p^{n+1}})$, on $\zeta_{p^{n+1}}$ és una arrel p^{n+1}-èssima de la unitat si p és senar, i una arrel 2^{n+2}-èssima de la unitat quan $p = 2$.

Demostració. Prenem una extensió L de grau p^n continguda en $\mathbb{Q}(\zeta_{p^{n+1}})$. El que aspirem a demostrar és que la composició KL també ho està. Sabem que $\mathrm{Gal}(L/\mathbb{Q})$ és cíclic per estar contingut en una extensió cíclica. Prenem τ un generador i $\widehat{\tau}$ una extensió d'aquest automorfisme a KL. Sigui F el cos fix de $\widehat{\tau}$. Com que el cos fix de τ és $\mathbb{Q}$, tenim $L \cap F = \mathbb{Q}$. Pels resultats habituals de teoria de Galois podem construir la injecció $\mathrm{Gal}(KL/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(K/\mathbb{Q})$, que implica que $\widehat{\tau}$ té ordre fitat per p^n, i en estendre un automorfisme de grau p^n tenim que el grau exacte de $\widehat{\tau}$ és p^n. Per tant, $[KL : F] = p^n$ i volem arribar a $KL = FL$, $FL \subset \mathbb{Q}(\zeta_{p^{n+1}})$ i finalment a $K \subset \mathbb{Q}$. Veurem que $[FL : F] = p^n$ separant en dos casos.
Cas $p = 2$) Considerem l'automorfisme de conjugació complexa. El seu cos fix haurà de contenir alguna extensió quadràtica, a no ser que sigui $\mathbb{Q}$. Com que partim de que el discriminant és una potència de 2, aquest cos ha de ser $\mathbb{Q}(\sqrt{2})$, que per un argument semblant també estarà en L, cosa que contradiu $L \cap F = \mathbb{Q}$. Per tant, el cos fix seran en els racionals. Per tant, $[F : \mathbb{Q}] = 2$ i F ha de ser $\mathbb{Q}(i)$ o $\mathbb{Q}(\sqrt{-2})$, ergo $FL = \zeta$ i $[FL : F] = 2^n$, que és el que volíem.
Cas p senar) Tenim una única subextensió cíclica de grau p i discriminant potència de p, tant a L, com a F, quan $F \neq \mathbb{Q}$. Però F era la fixa per un element que genera $\mathrm{Gal}(L/\mathbb{Q})$, el qual és sempre equivalent a $L \cap \mathbb{Q}$. Per tant, $F = \mathbb{Q}$ i tenim $FL = L \subset \mathbb{Q}(\zeta)$. Llavors $[FL : F] = [L : \mathbb{Q}] = p^n$. □

2 Cossos locals

Per a acostumar-nos als objectes amb els que estarem constantment tractant i al mateix temps fixar la notació, farem un breu repàs del que ens cal saber sobre cossos locals a l'hora d'abordar la teoria de cossos de classe local. La intenció és que gairebé sempre podrem agafar com a model el cos $\mathbb{Q}_p$.

2.1 Valors absoluts

Definició 2.1. Donat un cos K, una valor absolut és una aplicació $|\,| : K \to \mathbb{R}_{\geq 0}$ que compleix les següents propietats:

1. $|x| = 0$, si i només si, $x = 0$.
2. $|xy| = |x||y|$.
3. $|x + y| \leq |x| + |y|$.

També direm que aquesta valoració és no arquimediana o ultramètrica si compleix la propietat $|x + y| \leq \max(|x|, |y|)$.

Igual que en el cas d'espais vectorials les normes indueixen topologies, els valors absoluts també indueixen una distància en el cos, i per tant, una topologia. Quan tenim un valor absolut en un cos, podem usar el procediment de compleció per obtenir un nou cos, on totes les successions de Cauchy siguin convergents.

Exemple 2.1. Al cos dels nombres racionals podem definir el valor absolut real de la manera habitual. Al completar respecte aquest valor absolut obtenim el cos dels nombres reals $\mathbb{R}$.

També podem definir altres valors absoluts fent servir les anomenades valoracions discretes

Definició 2.2. Una valoració discreta en un cos K és una aplicació $v : K \to \mathbb{Z} \cup \{\infty\}$ complint les següents propietats:

1. $v(x) = \infty$, si i només si, $x = 0$.
2. $v(xy) = v(x) + v(y)$.
3. $v(x + y) \geq \min(v(x), v(y))$.

Podem definir una valoració en un context més general si a l'arribada posem un grup topològic que no estigui dotat necessàriament de la topologia discreta.

Exemple 2.2. Donat $a \in \mathbb{Q}$ i $p \in \mathbb{Z}$ un primer, podem escriure a de manera única com $a = \frac{m}{n}p^r$ on $m, n, r \in \mathbb{Z}$, $(m, n) = 1$ i $n > 0$. Definim la valoració p-àdica com $v_p(a) = r$.

Proposició 2.1. v_p compleix les propietats d'una valoració discreta i indueix un valor absolut no arquimedià donat per $|x|_p = p^{-v_p(x)}$.

Demostració. La primera propietat és immediata. També tenim que si $x = p^r \frac{a}{b}$ i $y = p^s \frac{a'}{b'}$, $xy = p^{r+s} \frac{aa'}{bb'}$, aleshores

$$v_p(xy) = r + s = v_p(x) + v_p(y).$$

Conseqüentment

$$|xy|_p = p^{-r-s} = p^{-r}p^{-s} = |x|_p|y|_p.$$

La desigualtat triangular es desprèn de la demostració de la propietat no-arquimediana. Si escrivim la suma de dos racionals $x = \frac{a}{b}$, $y = \frac{c}{d}$, tenim $x + y = \frac{ad+bc}{cd}$ i sabem que l'ordre d'una suma serà major o igual que l'ordre més petit.

$$\begin{aligned} v_p(x + y) &= v_p(ad + bc) - v_p(b) - v_p(d) \geq \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) \\ &= \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) = \min(v_p(x), v_p(y)) \end{aligned}$$

Així:

$$|x + y|_p = p^{-v_p(x+y)} \leq p^{-\min(v_p(x), v_p(y))} = \max(p^{-v_p(x)}, p^{-v_p(y)}) = \max(|x|_p, |y|_p).$$

□

Sovint també anomenarem ordres a aquestes valoracions i les notarem per ord_p.

Exemple 2.3. Al completar $\mathbb{Q}$ respecte una valoració d'aquest tipus obtenim el cos dels nombres p-àdics, que coincideix amb la definició donada a la secció introductòria. També és habitual definir aquest cos en termes de límits projectius.

Es pot demostrar que quan tenim un cos K complet respecte una valoració v_p, el seu anell d'enters coincideix amb

$$\mathcal{O}_K = \{x \in K \text{ amb } |x|_p \leq 1\} = \{x \in K \text{ amb } v_p(x) \geq 0\}.$$

Per la multiplicativitat de la norma, tindrem que les unitats d'aquest anell seran les que tinguin valoració 0. L'únic ideal maximal serà

$$\mathfrak{m}_K = \{x \in K \text{ amb } v_p(x) \geq 1\},$$

o el que és el mateix, els elements que tenen ordre estrictament positiu. Si aquest anell és un domini d'ideals principals podem escollir un generador w_v al que anomenarem uniformitzador. Aquest anell, a més, és un anell de valoració discreta, en el qual tot element s'escriu de manera única com uw_v^r, essent u una unitat. També usarem els cossos residuals, que són els quocients per l'ideal maximal,

$$k = \mathcal{O}_K/\mathfrak{m}_K.$$

Les notacions usades seran les habituals durant tot el desenvolupament.

Definició 2.3. Direm que dos valors absoluts són $|\,|, |\,|'$ són equivalents si existeix un $c \in \mathbb{R}$ tal que $|x| = |x|'^c$ per tot $x \in K$.

Teorema 2.1. (*Ostrowski*) A $\mathbb{Q}$, qualsevol valor absolut és equivalent a la norma habitual a $\mathbb{R}$ o bé a algun dels valors absoluts $|\,|_p$.

Demostració. Koblitz, p-adic NAF, 2 □

L'avantatge de pensar un cos en termes les seves valoracions és que els elements d'aquest cos es poden veure com elements en les completacions respecte cadascuna de les valoracions. Així, podem aproximar qualsevol element del cos per diversos elements en cada valoració. Aquesta idea es plasma en el teorema d'aproximació dèbil, que farem servir al llarg del treball.

Teorema 2.2. (*d'aproximació dèbil*) Siguin $v_1, \ldots, v_n$ valoracions no trivials i no equivalents entre elles en un cos K, i $a_1, \ldots, a_n$ elements diferents del cos. Per cada $\varepsilon > 0$, existeix un element $a \in K$ tal que $v_i(a - a_i) < \varepsilon$ per cada i.

Demostració. Milne, ANT, 7.20. □

Aquest resultat només valdrà quan tinguem n valoracions diferents, per exemple, a $\mathbb{Q}$, tindrem les valoracions indicades en el teorema d'Ostrowski. Quan completem un cos respecte una d'aquestes valoracions, parlarem de cos local.

Definició 2.4. Un cos local K_v és un cos complet i localment compacte respecte una valoració discreta. Hi ha tres tipus de cossos locals:

1. Cossos locals arquimedians: $\mathbb{R}$.
2. Cossos locals no-arquimedians de característica 0: $\mathbb{Q}_p$ i les seves extensions
3. Cossos locals no-arquimedians de característica p: $\mathbb{F}_p(T)$ i les seves extensions.

D'aquí en endavant ens centrarem en els cossos del segon tipus. Fixarem la notació dient que K_v és un cos local complet respecte una valoració no-arquimediana (l.c.a.). També cal dir, que les propietats topològiques jugaran un paper clau durant tot el treball, requerint que els cossos siguin localment compactes.

Proposició 2.2. Sigui K_v un cos local. Aleshores, $\mathcal{O}_L$ és compacte, si i només si, k és un cos finit.

Demostració. $\Rightarrow$) Sigui S un conjunt de representants de k_v. La compacitat de $\mathcal{O}_K$ ens indica que qualsevol recobriment obert ha de contenir un subrecobriment finit. Si el recobirement és disjunt, és a dir, els oberts no s'intersequen entre ells, aleshores ell mateix ha de ser finit. Prenem com a recobriment els oberts $s+\mathfrak{m}_{K_v}$ on $s \in S$, que és obert[4] i disjunt, i per tant finit.
$\Leftarrow$) Per veure que $\mathcal{O}_K$ és compacte veurem primer que és obert i tancat. És obert ja que al ser discreta la valoració existirà algun δ prou petit tal que $\mathcal{O}_K = \{x \in K \text{ amb } v(x) < 1+\delta\}$; i és tancat ja que

$$\mathcal{O}_K = \{x \in K \text{ amb } v(x) \leq 1\}.$$

Observem ara que

$$\mathcal{O}_K \cong \varprojlim \mathcal{O}_K/\omega^n\mathcal{O}_K \subset \prod \mathcal{O}_K/\omega^n\mathcal{O}_K$$

Les components $\mathcal{O}_K/\omega^n\mathcal{O}_K$ són finites, i per tant compactes (amb la topologia discreta). Això converteix a $\prod \mathcal{O}_K/\omega^n\mathcal{O}_K$ en compacte, usant el teorema de Tychonoff. Si veiem que $\mathcal{O}_K$ és tancat dins un espai compacte, haurem vist també que és compacte. Per veure això, veiem que el seu complementari és obert. Prenem $(x_n) \in \prod \mathcal{O}_K/\omega^n\mathcal{O}_K$ tal que existeixen r, s de manera que $x_r \not\equiv x_s \mod \omega^r$ amb $r < s$. Aleshores, podem construir un conjunt que contingui aquest punt de la manera

$$U = \prod_{n>s} \mathcal{O}_K/\omega^n\mathcal{O}_K \times \{x_s\} \times \cdots \times \{x_1\}$$

que és obert; clarament aquest entorn no pot intersecat $\mathcal{O}_K$. □

Usant l'estructura algebraica de K_v, podem veure que $s + \mathcal{O}_K$ és un entorn compacte de s, per tot $s \in K_v$, sempre i quan el cos residual k sigui finit. Això passarà sempre que K_v sigui una extensió finita de $\mathbb{Q}_p$, i en aquest cas sabrem que el cos és localment compacte amb la topologia induïda pel valor absolut.

Proposició 2.3. Sigui K_v un cos local no-arquimedià i sigui k_v el cos residual. Llavors

$$K_v^\times = \omega_v^{\mathbb{Z}} \times \mathcal{O}_K^\times,$$

amb ω un uniformitzador (element que genera l'ideal maximal).

Demostració. Sigui $\alpha \in K_v^\times$. Sabem que té una única represenvació en la forma $\alpha\omega_v^n$, el qual directament demostra $K_v = \omega^{\mathbb{Z}} \times \mathcal{O}_K^\times$. □

Cal remarcar que $\mathcal{O}_K^\times$ conté una part de torsió, és a dir, un subgrup d'elements amb ordre finit. Aquest subgrup serà interessant quan intentem comparar les extensions abelianes de K_v amb els subgrups de $K_v^\times$. Per exemple, a $\mathbb{Z}_p$, que és l'anell d'enters de $\mathbb{Q}_p$, les seves unitats $\mathbb{Z}_p^\times$ contenen el subgrup $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \mathbb{Z}/(p-1)\mathbb{Z}$ com a subgrup de torsió.

2.2 Extensions de les valoracions

Una pregunta força evident que sorgeix del desenvolupament dels cossos locals és què pot passar amb les valoracions quan prenem una extensió finita de cossos locals. És a dir, si donada una valoració v en un cos local K i una extensió L finita d'aquest cos podem trobar una valoració a L que sobre ens elements de K es mantingui igual. Per fer això, refrescarem la idea de norma de teoria de Galois.

Definició 2.5. Donada una extensió finita de Galois L/K de grau n, podem definir la norma $\mathrm{Nm}_{L/K} : L^\times \to K^\times$ de les tres maneres equivalents següents.

1. Sigui $\alpha \in L^\times$; la multiplicació per α és un endomorfisme d'espais vectorials sobre K representat per la matriu A_α. Podem definir $\mathrm{Nm}_{L/K}(\alpha) = \det(A_\alpha)$.
2. Sigui $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ el polinomi mínim de α. Aleshores, $\mathrm{Nm}_{L/K}(\alpha) = (-1)^n a_0$.
3. Sigui G el grup de Galois de l'extensió. Aleshores, $\mathrm{Nm}_{L/K}(\alpha) = \prod_{\sigma\in G} \sigma(\alpha)$.

Es defineix una valoració w sobre el cos L usant la fórmula $w(\alpha) = v(\mathrm{Nm}_{L/K}(\alpha))^{\frac{1}{n}}$.

[4] Si U és un obert i $x \in K_v$, és immediat veure que $x + U$ també serà obert

Proposició 2.4. w és una valoració i $w(\alpha) = v(\alpha)$ per $\alpha \in K$. Diem que és una extensió de la valoració.

Demostració. Primer veiem que w és una extensió. Sabem que els elements de K queden fixos pel grup de Galois que té n elements. Així $\mathrm{Nm}_{L/K}(\alpha) = \alpha^n$ si $\alpha \in K$ i conseqüentment $w(\alpha) = v(\alpha^n)^{\frac{1}{n}} = v(\alpha)$. Ara veurem les tres propietats de valoració.

1. $w(x) = 0$, implica $v(\mathrm{Nm}_{L/K}(x)) = 0$, i per tant $\mathrm{Nm}_{L/K}(x) = 0$, que només passa quan $x = 0$.
2. La multiplicativitat es segueix la multiplicativitat de la norma.
3. Volem provar que si $w(\beta) \geq w(\alpha)$, aleshores $w(\alpha + \beta) \leq w(\beta)$; això equival a veure que $w(1 + \frac{\alpha}{\beta}) \leq 1$. Per tant, hem de demostrar que si $w(\gamma) \leq 1$, aleshores $w(1 + \gamma) \leq 1$, que és clarament cert.

□

2.3 Extensions totalment ramificades

Ara anem a veure quines són les possibilitats de la ramificació en aquest tipus de cossos. Sembla evident que serà més fàcil que en un cos de nombres ja que només tenim un sol ideal primer $\mathfrak{m}_K$.

Definició 2.6. Un polinomi $f(x) \in K[X]$ és $\mathfrak{p}$-Einsenstein per a algun ideal primer $\mathfrak{p} \subset \mathcal{O}_K$ si $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ amb $a_i \in \mathfrak{p}$, i $a_0 \notin \mathfrak{p}^2$. Així una extensió L/K_v és Einsenstein si es construeix afegint una arrel α d'un polinomi d'Eisenstein, $L = K_v(\alpha)$.

Ens proposem demostrar que aquestes extensions són les mateixes que les totalment ramificades, aquelles on l'ideal maximal ramifica completament i per tant l'extensió de cossos residuals l/k és trivial.

Teorema 2.3. Sigui K_v un cos no-arquimedià local. Una extensió L/K_v és totalment ramificada, si i només si, és $\mathfrak{m}_K$-Einsenstein.

Demostració. $\Leftarrow$) Sigui $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathcal{O}_K[x]$ el polinomi d'Einsenstein separable en qüestió. Siguin $\alpha_1, \ldots \alpha_n$ les seves arrels en alguna clausura algebraica (α_i la que genera la nostra extensió) i ω un uniformitzador. Totes les arrels tenen la mateixa norma, i $a_0 \in \mathfrak{m}_v^2 - \mathfrak{m}_v$. Per tant:

$$|\alpha_i|^n = \prod_i |\alpha_i| = |a_0| = |\omega|$$

Sigui e l'index de ramificació, $f = [l : k]$ i ω_L un uniformitzador de l'extensió. Sabem que $\omega = \omega_L^e u$ i $\alpha_i = \omega_L^f v$ amb u, v dues unitats de l'anell d'enters. També recordem que com que només hi ha un ideal primer, tindrem $ef = n$. Per tant,

$$|\omega|^{\frac{1}{n}} = |\alpha_i| = |\omega_L|^f = |\omega|^{\frac{f}{e}}.$$

Amb això, $n = \frac{e}{f} \leq e$ i conseqüentment, $e = n$ i $f = 1$, com volíem veure.
$\Rightarrow$) Podem agafar un uniformitzador de l'extensió, ω_L, i $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \in \mathcal{O}_K[x]$ el seu polinomi mínim. Els seus conjugats ω_i tindran la mateixa norma, que és $|\omega_i| < 1$. Com que els a_i són polinomis simètrics avaluats en les arrels també compliran $|a_i| < 1$, i per tant pertanyeran a $\mathfrak{m}_v$. Només falta veure que a_0 no està en $\mathfrak{m}_v^2$. Ja hem usat anteriorment que $|a_0| = |\omega_l|^n = |\omega|$, i llavors $a_0 = u\omega$, que és suficient per veure-ho. □

2.4 Extensions no ramificades

Definició 2.7. Una extensió L/K és no ramificada si l'índex de ramificació de l'ideal maximal és $e = 1$.

En aquest cas, en comptes de donar una caracterització directa d'aquests cossos, posarem totes les extensions no ramificades en bijecció amb les subextensions finites dels cossos residuals. També obtindrem un bon comportament respecte als grups de Galois dels nostres cossos.

Teorema 2.4. Existeix una bijecció entre les extensions no ramificades finites i separables de cossos locals i les extensions finites del cos residual k. A més, es compleixen les següents propietats:

1. La bijecció respecta les inclusions de cossos. Si $L_1 \subset L_2$, aleshores $l_1 \subset l_2$.

2. Els grups de Galois són els mateixos: $\mathrm{Gal}(L/K) = \mathrm{Gal}(l/k)$.

Teorema 2.5. Sigui L/K una extensió d'un cos local. Són equivalents les següents condicions:

1. L/K és no ramificada.
2. $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ és un cos.
3. $[L:K] = [l:k]$.
4. Si ω_K un uniformitzador a $\mathcal{O}_K$, també ho serà a $\mathcal{O}_L$.
5. El subgrup d'inèrcia $I_{\mathfrak{m}}$ és trivial.

Demostració. 1) $\Rightarrow$ 2) L'ideal maximal continua sent-ho a $\mathcal{O}_L$. Per tant, $\mathcal{O}_L/\mathfrak{m}_K\mathcal{O}_L$ és quocient per un ideal maximal i com a tal és un cos.
2) $\Rightarrow$ 3) En la fórmula $ef = n$ tenim que $e = 1$ i per tant $f = n$.
3) $\Rightarrow$ 4) En la fórmula del teorema 2.2, tenim $f = n$, i conseqüentment $e = 1$. Per tant, l'ideal maximal seguirà sent-ho i el mateix uniformitzador seguirà valent.
4) $\Rightarrow$ 5) Les condicions em donen que $e = 1$, i e és precissament l'ordre de la inèrcia.
5) $\Rightarrow$ 1) L'ordre del subgrup d'inèrcia és $e = 1$, i llavors l'extensió és no ramificada. □

Gràcies a que sabem que, fixat un grau, existeix una única extensió de cossos finits amb aquell grau, que és cíclica i generada per l'element de Frobenius, podem deduir que existeix una única extensió no ramificada de grau n d'un cos local per a tot $n \geq 0$.

2.5 Extensions quadràtiques de $\mathbb{Q}_p$

Recordem que dues extensions quadràtiques $\mathbb{Q}_p(\sqrt{a}) = \mathbb{Q}_p(\sqrt{b})$ seran iguals si $\frac{a}{b} \in (\mathbb{Q}_p^\times)^2$. Per tant, hi haurà tantes extensions quadràtiques com elements a $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ no trivials. Ara, intentem buscar quin és aquest nombre, observant que

$$(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}.$$

Tenim l'isomorfisme

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong (\mathbb{Z}_{\text{ı}}^\times \times \mathbb{Z})/((\mathbb{Z}_p^\times)^2 \times 2\mathbb{Z}) \cong \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \times \mathbb{Z}/2\mathbb{Z}.$$

Recordi's que hi ha una successió exacta curta

$$0 \to \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times \to \mathbb{Z} \to 0,$$

que indueix una descomposició natural

$$\mathbb{Q}_p^\times \simeq \mathbb{Z}_p^\times \times \mathbb{Z};$$

però, per definir l'isomorfisme s'ha de fer una tria d'un uniformitzador (és a dir, no está definit de forma natural). A més, si $p \neq 2$, $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times (1 + p\mathbb{Z}_p)$, amb $\pi : \mathbb{Z}_p^\times \twoheadrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ la projecció sobre el primer factor. Si $p = 2$, $\mathbb{Z}_2^\times \simeq (\mathbb{Z}/2\mathbb{Z}) \times (1 + 4\mathbb{Z}_2)$ i definim de la mateixa manera el morfisme π.

Sabem que $p\mathbb{Z}_p$ és l'ideal maximal de $\mathbb{Z}_p$, i per tant $\operatorname{Ker}\pi = 1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ (quan $p = 2$ el nucli serà $1 + 4\mathbb{Z}_2$). A més, si $p \neq 2$, es pot demostrar que $\left(1 + p\mathbb{Z}_p\right)^2 = 1 + p\mathbb{Z}_p$ veient que qualsevol enter p-àdic es pot escriure com $2x + px^2$ si $p \neq 2$ i observant que $(1 + px)^2 = 1 + (2x + px^2)p$[5]. En aquest cas,

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong (\mathbb{Z}/p\mathbb{Z})^\times/((\mathbb{Z}/p\mathbb{Z})^\times)^2 \cong \mathbb{Z}/2\mathbb{Z}$$

Amb això ja tenim $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ i obtenim tres extensions quadràtiques. Les extensions de grau primer sempre seran totalment ramificades o no ramificades, ja que $ef = n$ amb n primer. N'hi ha una única de no ramificada, i la resta són totalment ramificades.

[5] El procediment general per a trobar solucions de les equacions polinòmiques a $\mathbb{Z}_p$ es diu lema de Hensel, que a partir de solucions mòdul p^r en genera d'altres mòdul p^{r+1}.

Exemple 2.4. Per $p = 5$, considerem les extensions $\mathbb{Q}_5(\sqrt{-1}), \mathbb{Q}_5(\sqrt{2}), \mathbb{Q}_5(\sqrt{3}), \mathbb{Q}_5(\sqrt{5}), \mathbb{Q}_5(\sqrt{10})$. De totes aquestes veiem quines són iguals o trivials. Usant el símbol de Legendre veiem que $\left(\frac{-1}{5}\right) = 1$, que implica que $\mathbb{Q}_5(\sqrt{-1}) = \mathbb{Q}_5$. Idènticament, $\left(\frac{2}{5}\right)\left(\frac{3}{5}\right) = 1$, amb el qual $\mathbb{Q}_5(\sqrt{2}) = \mathbb{Q}_5(\sqrt{3})$. Seguint amb aquests arguments arribem a que les úniques no isomorfes ni trivials són: $\mathbb{Q}_5(\sqrt{2}), \mathbb{Q}_5(\sqrt{5}), \mathbb{Q}_5(\sqrt{10})$. Els seus discriminants són $8, 5, 40$ i l'única en que 5 no ramifica és $\mathbb{Q}_5(\sqrt{2})$.

En el cas $p = 2$, hem de veure qui és $(\mathbb{Z}_2^\times)^2 = (\mathbb{Z}/4\mathbb{Z})^\times \times (1+4\mathbb{Z}_2)^2$. En aquest cas, $(1+4x)^2 = 1+8x+16x^2$ i llavors $(1 + 4\mathbb{Z}_2)^2)$ té índex 2 a $1 + 4\mathbb{Z}$, ja que la condició necessària i suficient per a que un nombre a $\mathbb{Z}_2$ es pugui representar com $2x + 4x^2$ és que sigui parell. Aleshores, $(1 + 2\mathbb{Z}_2)^2 = 1 + 8\mathbb{Z}_2$. Amb això tindrem l'isomorfisme

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Hi ha 7 extensions quadràtiques, de les quals només una pot ser no ramificada.

Exemple 2.5. En els termes en que hem construit l'últim isomorfisme les adjuncions que hem de fer són arrels del polinomi $X^2 - d$ amb d de la forma $(1 + a_1 2 + a_2 2^2)2^{a_3}$ que dónen lloc a les extensions $\mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{3}), \mathbb{Q}_2(\sqrt{5}), \mathbb{Q}_2(\sqrt{6}), \mathbb{Q}_2(\sqrt{7}), \mathbb{Q}_2(\sqrt{10}), \mathbb{Q}_2(\sqrt{14})$ i la única no ramificada és $\mathbb{Q}_2(\sqrt{5})$ perquè té discriminant 5 que és l'únic discriminant senar.

3 Cohomologia de grups

L'objectiu d'aquesta secció és construir una eina matemàtica prou potent per a poder demostrar els resultats de la teoria de cossos de classe per al cas de cossos locals, i també la farem servir en l'estudi del cas global. El tipus de desenvolupaments es fonamenten sobre l'àlgebra homològica, però en comptes de usar grups abelians, la nostra eina seran els G-mòduls. Per a que ens serveixi de motivació, generalment estarem pensant en grups multiplicatius de cossos, sobre els quals actúa el grup de Galois.

3.1 G-mòduls

Definició 3.1. Sigui G un grup. Direm que M és un G-mòdul si M és un grup abelià amb una operació:

$$G \times M \to M$$

que compleix:

$$g(m_1 + m_2) = gm_1 + gm_2;$$
$$(g_1 g_2)m = g_1(g_2 m).$$

Aquí hem escrit l'operació de G amb notació multiplicativa i la de M amb notació additiva. Tot i així, en cas que la operació de M sigui multiplicativa escriurem ${}^g m$ per representar l'operació. Això passarà habitualment quan prenguem com G un grup de Galois, i M algun tipus de subgrup multiplicatiu.

Exemple 3.1. Sigui L/K una extensió galoisiana de cossos i G el seu grup de Galois. Podem dir que G actua sobre el grup multiplicatiu de l'extensió $L^\times$ com un G-mòdul. Idènticament actuaria sobre el grup de classes, el grup d'ideals fraccionaris o les unitats de l'anell d'enters de l'extensió.

A priori, semblaria que la noció de mòdul que hem donat es pot confondre amb la noció de mòdul com a espai vectorial sobre un anell. Observem, però, que donat un grup G, es pot definir el següent anell:

$$\mathbb{Z}[G] = \Big\{ \sum_i n_i g_i \,|\, n_i \in \mathbb{Z}, g_i \in G \Big\}.$$

La noció de G-mòdul coincideix amb la de mòdul sobre aquest anell. De fet, com que definim aquesta estructura sobre un grup abelià, podem introduir un producte i llavors solem anomenar-la àlgebra de grup. Una vegada hem establert això, podem definir un morfisme de G-mòduls de manera que es respectin les operacions.

Definició 3.2. Diem que la aplicació $\phi : M \to N$ és un morfisme de G-mòduls si és un morfisme de grups que compleix la següent propietat.

$$\phi(gm) = g\phi(m) \; \forall g \in G$$

Denotem com $\mathrm{Hom}_G(M, N)$ tots els morfismes entre M i N.

Exemple 3.2. Suposem que el grup de Galois G d'una extensió L/K és cíclic d'ordre n generat per un automorfisme σ. La aplicació $\Delta(a) = \frac{a}{\sigma(a)}$ és un endomorfisme de $L^\times$ com a G-mòdul. També l'aplicació norma habitual en el cos L ho és.

Definició 3.3. Direm que I és un G-mòdul injectiu si el functor $\mathrm{Hom}(\cdot, I)$ és exacte.

El functor que hem definit agafa G-mòduls i els envia a conjunts d'morfismes (que també es poden pensar com a G-mòduls). Diem que és exacte si donada la successió exacta de G-mòduls

$$0 \to M_1 \to M_2 \to M_3 \to 0,$$

aleshores la successió

$$0 \to \mathrm{Hom}(M_3, I) \to \mathrm{Hom}(M_2, I) \to \mathrm{Hom}(M_1, I) \to 0$$

també és exacta. Es pot demostrar que qualsevol G-mòdul està contingut dins algun mòdul injectiu.

3.2 Una mica d'àlgebra homològica

Durant el transcurs del treball també requerirem usualment els dos següents lemes d'àlgebra homològica, que seran usats en repetides ocasions per a construir successions exactes d'homomorfismes que ens siguin útils. Enunciarem aquests dos resultats per a grups però es pot demostrar que l'estructura de G-mòdul també quedarà fixa. De fet, durant la secció trobarem explícitament alguns dels morfismes que apareixen implícitament durant aquest parèntesi d'àlgebra homològica, per als grups de cohomologia.

Lema 3.1. (de la serp) Donat un diagrama de morfismes de grups amb files exactes

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f} & B' & \xrightarrow{g} & C' & & \end{array}$$

podem construir una successió exacta de morfismes

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} a \to \operatorname{Ker} b \to \operatorname{Ker} c \to \operatorname{Coker} a \to \operatorname{Coker} b \to \operatorname{Coker} c \to \operatorname{Coker} g' \to 0.$$

Per demostrar aquest resultat hem de caçar en l'esquema inicial en cada pas per a construir la successió. La única aplicació que té una certa dificultat en la definició és la intermèdia entre el nucli i el conucli, també anomenada morfisme de connexió.

Lema 3.2. (nucli-conucli) Donats dos morfismes de grups abelians

$$A \xrightarrow{f} B \xrightarrow{g} C\ ,$$

existeix una successió exacta llarga

$$0 \to \operatorname{Ker} f \to \operatorname{Ker} g \circ f \to \operatorname{Ker} g \to \operatorname{Coker} f \to \operatorname{Coker} g \circ f \to \operatorname{Coker} g \to 0.$$

Per demostrar aquest segon resultat només hem d'aplicar el lema de la serp al diagrama

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \longrightarrow & \operatorname{Coker} f & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle g\circ f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle c} & & \\ 0 & \longrightarrow & C & \longrightarrow & C & \longrightarrow & 0 & & \end{array}$$

□

3.3 Grups de cohomologia

Definició 3.4. Definim la resolució injectiva de M com una successió exacta llarga de G-mòduls de la forma següent

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \to \dots,$$

on cada aplicació és la inclusió dins un mòdul injectiu.

Definició 3.5. Donat M un G-mòdul, podem definir el grup abelià

$$M^G = \{m \in M \mid gm = m \quad \forall g \in G\}.$$

És a dir, els elements de M fixats per G.

La aplicació que envia M a M^G és un functor dins la categoria dels G-mòduls. Podem fer servir aquest functor per obtenir una nova successió de G-mòduls

$$0 \xrightarrow{d^{-1}} I_0^G \xrightarrow{d^0} I_1^G \xrightarrow{d^1} \dots$$

A més, no serà necessàriament exacta, per tant podem definir els grups de cohomologia a partir dels seus nuclis i imatges.

Definició 3.6. Sigui $r \geq 0$. El r-èssim grup de cohomologia de M sobre G es defineix com

$$H^r(G, M) = \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}.$$

Si només tenim definida una part de la resolució, podem definir així els primers grups de cohomologia.

Es relativament senzill veure que un morfisme ϕ entre dos G-mòduls A i B indueix trivialment un altre morfisme entre els grups de cohomologia entre $H^r(G, A), H^r(G, B)$ [2]. La unicitat d'aquestes resolucions injectives es dóna llevat d'equivalència homotòpica. En altres paraules, si tenim dues resolucions injectives que denotarem per I_i i J_i, aleshores tenim un diagrama commutatiu entre les dues de la forma

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{d^{-1}} & I_0 & \xrightarrow{d_0} & I_1 & \longrightarrow & \dots \\ & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M & \xrightarrow{d^{-1}} & J_0 & \xrightarrow{d^0} & J_1 & \longrightarrow & \dots \end{array}$$

A priori no és evident que a partir d'aquesta relació obtinguem una identificació entre els grups de cohomologia. Per a veure-ho, necessitem introduir la noció d'equivalència homotòpica entre les dues successions, dient que existeixen morfismes

$$T_i : J_i \to I_{i-1}$$

de manera que $d^{i-1} \circ T_i - T_{i+1} \circ d^i = d^{i-1}m$ per algun $m \in I_i$. Aquesta noció d'homotopia ens permet veure que els grups definits per cadascuna de les dues successions seràn els mateixos. A aquest fet l'anomenem invariància homotòpica de la cohomologia de G-mòduls.

Portem al nostre exemple anterior aquestes definicions.

Exemple 3.3. Sigui G el grup de Galois d'una extensió L/K cíclica d'ordre n generada per σ. Aleshores podem definir la següent successió:

$$1 \to L^\times \xrightarrow{\Delta} L^\times \xrightarrow{N} L^\times \xrightarrow{\Delta} L^\times \dots$$

on $\Delta = \mathrm{id}\,/\sigma$ i $N = \prod_i \sigma_i$. Notem que és un complex atès que

$$\Delta(N(a)) = \frac{\prod_i^{\sigma^i} a}{\prod_i^{\sigma^{i+1}} a} = 1,$$

$$N(\Delta(a)) = \prod_i \frac{{}^{\sigma^i}a}{\sigma^{i+1}a} = 1.$$

Això implica que $\mathrm{Im}\, N \subset \mathrm{Ker}\, \Delta$ i que $\mathrm{Im}\, \Delta \subset \mathrm{Ker}\, N$. Per tant, podrem definir els primers grups de cohomologia.

$$H^0(G, M) = \frac{\mathrm{Ker}(\Delta)}{\mathrm{Im}(N)};$$

$$H^1(G, M) = \frac{\mathrm{Ker}(N)}{\mathrm{Im}(\Delta)}.$$

Podem fer una primera llista de propietats bàsiques dels grups de cohomologia.

Proposició 3.1. Las següents propietats es donen en els grups de cohomologia.

1. $H^0(G, M) = M^G$
2. $H^r(G, I) = 0$ si I és un mòdul injectiu $\forall r \geq 0$.

[2] De fet s'indueixen seqüencies llargues a partir de curtes de la mateixa manera que en homologia

3. Qualsevol successió de G-mòduls
$$0 \to M_1 \to M_2 \to M_3 \to 0$$
indueix una successió en els grups de cohomologia.
$$\cdots \to H^r(G, M_1) \to H^r(G, M_2) \to H^r(G, M_3) \xrightarrow{\delta} H^{r+1}(G, M_1) \to \dots$$
$$\dots H^{r+1}(G, M_2) \to H^{r+1}(G, M_3) \to \dots$$

Demostració. 1. Identifiquem en primer lloc $\mathrm{Ker}(d^0)$. Podem pensar la successió donada pel functor $(\cdot)^G$ com una restricció de la resolució injectiva; per tant al estar incloent M^G dins I_0^G en una successió exacta tenim que el nucli és la imatge de la inclusió, és a dir M^G.

2. Si partim d'un mòdul injectiu tots els elements de la resolució seran el mateix. Com a tal, tots els nuclis i imatges seran iguals.

3. És el pas habitual d'una successió curta a una llarga en àlgebra homològica. Podem definir δ caçant en els diagrames. En el següent lema, ho fem explícitament per als primers grups de cohomologia.

□

Lema 3.3. (*L'hexàgon exacte*) Sigui
$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0,$$
amb A, B, C G-mòduls i f, g G-morfismes. Existeixen aplicacions δ_0, δ_1 que donen el següent diagrama:
$$\begin{array}{ccccc} H^0(G,A) & \xrightarrow{f_0} & H^0(G,B) & \xrightarrow{g_0} & H^0(G,C) \\ \uparrow \delta_1 & & & & \downarrow \delta_0 \\ H^1(G,C) & \xleftarrow{f_1} & H^1(G,B) & \xleftarrow{g_1} & H^1(G,A) \end{array}$$

Demostració. Ens fa falta definir δ_0 i δ_1 en els grups de cohomologia. Suposem que G és un grup de Galois cíclic. Sigui $[c] \in H^0(G, C)$. Com que g és exhaustiva, existeix $b \in B$ tal que $g(b) = c$. Aleshores $\Delta g(b) = g(\Delta b) = \Delta c = 1$, per tant $\Delta b \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Existeix $a \in A$ tal que $f(a) = \Delta b$. De nou, $f(N(a)) = N(f(a)) = N(\Delta b) = 1$ que implica $N(a) \in \mathrm{Ker}(f) = 1$ i $a \in \mathrm{Ker}(N)$. Ja estem en condicions de definir
$$\delta_0(c + N(C)) = a + \Delta A.$$
Definiriem δ_1 de manera anàloga. □

Lema 3.4. Sigui M_i una col·lecció de G-mòduls. Llavors $\prod_i M_i$ és també un G-mòdul i la seva cohomologia és $H^r(G, \prod_i M_i) = \prod_i H^r(G, M_i)$.

Demostració. Definim la acció sobre $\prod_i M_i$ com $g(m_1, m_2, m_3, \dots) = (gm_1, gm_2 m, gm_3, \dots)$ i la resolució projectiva seria la següent.
$$0 \to \prod_i M_i \xrightarrow{\prod_i d_i^1} \prod_i I_i^0 \to \dots$$

□

Ja tenim la maquinària de la cohomología definida. Tenim $H^0(G, M)$ caracteritzat i també els morfismes entre G-mòduls. Per a les successions que ens interessaran en la teoria de cossos de classe, també ens cal caracteritzar $H^1(G, M)$. Això ens permetrà presentar també els conceptes de cocicle i covora, que són claus per entendre la cohomologia.

Definició 3.7. Sigui $\phi : G \to M$ un morfisme. Direm que és un cocicle (o morfisme creuat) si compleix que $\phi(g_1 g_2) =^{g_1} \phi(g_2)\phi(g_1)$. Sigui ϕ un cocicle; si existeix $m \in M$ amb $\phi(g) = \frac{^g m}{m}$, direm que és una covora (o morfisme creuat principal).

Denotarem $\mathrm{Hom}(G, M)$ el conjunt dels morfismes, $Z(G, M)$ el conjunt dels cocícles i $B(G, M)$ el conjunt dels colimits.

Proposició 3.2. Els cocícles i colímits compleixen.

1. Els morfismes de G en M formen un grup amb el producte, del qual els cocicles i colimits en són subgrups.

2. $H^1(G,M) = \frac{Z(G,M)}{B(G,M)}$.

3. Si l'acció de G és trivial aleshores, $H^1(G,M) = \mathrm{Hom}(G,M)$.

Demostració. 1. Prendrem com l'aplicació identitat $\mathrm{id}(g) = \mathrm{id}_M$, i la inversa serà $\phi^{-1}(g) = (\phi(g))^{-1}$.
En el cas dels cocicles, la identitat és un cocicle $\mathrm{id}(g_1g_2) =^{g_2} (\mathrm{id}_M)\,\mathrm{id}_M = \mathrm{id}_M$ i el producte de dos cocícles és $\phi_1\phi_2(g_1g_2) =^{g_1} (\phi_1(g_2))\phi_1(g_1)^{g_1}(\phi_1(g_2))\phi_2(g_1) =^{g_1} (\phi_1\phi_2(g_2))\phi_1\phi_2(g_1)$; i finalment l'aplicació inversa és $\phi^{-1}(g_1g_2) =^{g_1} \phi^{-1}(g_2)\phi(g_2)$.
En el cas de les covores, la identitat és una covora donada per $m = \mathrm{id}_M$, el producte també (donat pel producte de les m) i la inversa, el mateix. El més interessant és veure que tota covora és un cocícle.

$$\phi(g_1g_2) = \frac{g_1g_2(m)}{m} = \frac{g_1g_2(m)}{g_1(m)}\frac{g_1(m)}{m} =^{g_1} (\phi(g_2))\phi(g_1)$$

Com que els grups són abelians, aquest subgrup serà abelià.

2. Sobre qualsevol mòdul M podem definir la successió següent [6]:

$$C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} C^2(G,M) \xrightarrow{d^2} \dots$$

on $C^r(G,M)$ són les aplicacións de $G^r \to M$ tals que $\phi(gg_1,\dots,gg_n) =^g \phi(g_1,\dots,g_n)$ i d^r definida com les aplicacions

$$d^r(\phi)(g_1,\dots,g_{r+1}) =^{g_1} \phi(g_2,\dots,g_{r+1}) + \sum_{j=1}^{r}(-1)^j\phi(g_1,\dots,g_jg_{j+1,\dots,g_{r+1}}) + (-1)^{r+1}\phi(g_1,\dots,g_r).$$

Es pot comprovar que per al cas $r = 1$, $\mathrm{Ker}(d^1) = Z(G,M)$ i $\mathrm{Im}(G,M) = B(G,M)$, amb el que obtindriem el resultat.

3. En el cas que l'acció de G sigui trivial, tots els morfismes són cocicles i l'única covora és la aplicació identitat.

□

Aquesta mateixa idea que apareix en la demostració de la segona part es pot usar per pensar quina forma tenen tots els grups d'ordre major. En particular la successió definida sobre les aplicacions $C^r(G,M)$, que anomenarem r-cocadenes no homogènies i la successió serveix com a resolució injectiva, gràcies a que $C^0(G,M) = M$. Per al nostre propòsit ens interessa especialment saber com és $H^2(G,M)$.

Exemple 3.4. Sigui M un G-mòdul. Necessitem coneixer les aplicacions d^2 i d^1

$$d^2(\phi)(g_1,g_2,g_3) =^{g_1} \phi(g_2,g_3) - \phi(g_1g_2,g_3) + \phi(g_1,g_2g_3) - \phi(g_1,g_2)$$

$$d^1(\phi)(g_1,g_2) =^{g_1} \phi(g_2) - \phi(g_1g_2) + \phi(g_1)$$

Idènticament a com hem definit abans $H^1(G,M)$, podem definit $H^2(G,M)$ com el quocient dels morfismes $\phi : G^2 \to M$ que compleixen $\phi(g_1,g_2) = \phi(g_1g_2,g_1g_3) + \phi(g_1,g_2g_3) - \phi(g_1g_2,g_3)$ per tot $g_3 \in G$, per la imatge de d^1, que coincideix amb aquells morfismes $\phi : G^2 \to M$ tals que existeix un morfisme $\psi : G \to M$ amb $\phi(g_1,g_2) = \psi(g_1)$.

[6] Aquesta podria haver estat una definició més precisa de la cohomologia però he pres la anterior que la escriu en termes de resolucions projectives i mòduls injectius. *Brown, LCFT, 3*

3.4 El lema de Shapiro

Definició 3.8. Sigui $H \subset G$ i sigui M un H-mòdul. Prenem el següent conjunt, al que anomenarem de mòduls induïts:

$$\mathrm{Ind}_H^G(M) = \{\phi : G \to M \mid \phi(hg) = h\phi(g) \quad \forall h \in H\}$$

No estem exigint que aquestes aplicacions siguin morfismes, però sí que podem notar que sobre el conjunt hi ha una estructura de G-mòdul. Aquesta estructura induïda també es comportarà bé amb els morfismes, i és el G-mòdul més petit que podem construir a partir d'un H-mòdul. És a dir, donat $\alpha : M \to M'$ morfisme de H-mòduls, l'aplicació $\phi \to \phi \circ \alpha$ serà un morfisme entre els G-mòduls induïts. Això permet intuir que tindrem un cert functor entre les categories de H-mòduls i G-mòduls al que podriem anomenar functor induit.

Lema 3.5. Prenem M un G-mòdul i N un H-mòdul, aleshores:

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(M, N)$$

Demostració. Per a cada G-morfisme $\alpha : M \to Ind_H^G(N)$, definim la següent aplicació $\beta : M \to N$ com:

$$\beta(m) = \alpha(m)(1_G)$$

que és un morfisme de H-mòduls. La aplicació $\psi(\alpha) = \beta$ és un morfisme respecte M i és bijectiva. □

Lema 3.6. *(Shapiro)* Sigui $H \subset G$ un subgrup G. Per qualsevol H-mòdul N, tenim el següent isomorfisme:

$$H^r(G, \mathrm{Ind}_H^G(N)) \simeq H^r(H, N)$$

Demostració. En el cas $r = 0$, apliquem el resultat anterior a M i $\mathbb{Z}$, pensant en $\mathbb{Z}$ com a G-mòdul amb l'acció trivial, ens dóna l'isomorfisme

$$\mathrm{Hom}_G(\mathbb{Z}, G) \cong M^G$$

que equival al teorema. Per a $r > 0$, es pot veure que el functor Ind_H^G és exacte. □

Una aplicació directa del lema de Shapiro és veure que la cohomologia del grup additiu d'un cos és nul·la.

Corol·lari 3.1. Sigui $\{0\}$ el subgrup trivial del grup de Galois G d'una extensió L/K finita. Llavors,

$$H^r(G, L) \simeq H^r(G, \mathrm{Ind}_0^G(K)) \simeq H^r(0, K) = 0.$$

Demostració. Si veiem que $L \cong \mathrm{Ind}_0^G(K)$, ja tindrem el resultat ja que el segon isomorfisme el segueix del lema de Shapiro. Primer de tot, recordant el teorema de la base normal sabem que per a algun $\alpha \in L$, els $\sigma(\alpha)$ seran base de L/K, per $\sigma \in G$. Per tant, podem pensar L com combinacions del grup de Galois a coeficients a K, que és el que es coneix com a àlgebra de grup, és a dir

$$K[G] = \Big\{ \sum_\sigma k\sigma \mid k \in K\ \sigma \in G \Big\}.$$

Ara construïm un isomorfisme entre $\mathrm{Ind}_0^G(K)$ i l'àlgebra enviant cada morfisme ϕ a una combinació sobre tots els elements de $K[G]$ del tipus $\sum_{g \in G} \phi(g^{-1})g$. Només cal veure que això és una bijecció. Com que no estem exigint cap condició sobre el morfisme ϕ podem construir-ne un per a que ens doni qualsevol element de l'àlgebra, i a més el 0 sempre anirà al 0. □

Corol·lari 3.2. (Teorema 90 de Hilbert) Sigui L/K una extensió de Galois finita amb grup de Galois G. Aleshores $H^1(G, L^\times) = 0$. Aquest resultat equival a dir que en una extensió cíclica generada per σ, un element $\beta \in L^\times$ té $\mathrm{Nm}(\beta) = 1$, si i només si, existeix $\alpha \in L^\times$ amb $\beta = \frac{\alpha}{\sigma(\alpha)}$.

Demostració. Prenem un cocícle ϕ i veiem que també és una covora. Per qualsevol $x \in L^\times$, sigui

$$y = \sum_{g \in G} \phi(g)g(x) = \phi(g_1)^{-1}y.$$

Si prenem $g_1 \in G$, aleshores

$$g_1 y = \sum_{g \in G} g_1 \phi(g) g(x) = \sum_{g \in G} \phi(g_1)^{-1} \phi(g_1 g) g_1 g(x).$$

Amb això tenim que ϕ és una covora generada per y^{-1} ja que $\phi(g_1) = \frac{y}{g_1(y)} = \frac{g_1(y^{-1})}{y^{-1}}$.
Per veure l'equivalencia amb el resultat clàssic de teoria de Galois, veiem que usant la resolució projectiva de l'exemple 3.3, els elements de norma 1 són el nucli de la aplicació norma, i els elements $\beta = \frac{\alpha}{\sigma(\alpha)}$ són la imatge de la aplicació Δ. □

Assumint el lema de Shapiro podem associar una aplicació entre la cohomologia d'un grup i un subgrup seu, de la següent manera. Donada la aplicació inclusió $i : H \hookrightarrow G$, volem introduir-la dins de la cohomologia. Si prenem les dues successions a partir de les quals definim la cohomologia d'un mòdul M en G i H, la inclusió defineix una única aplicació a la que anomenarem restricció

$$\mathrm{Res} : H^r(G, M) \to H^r(H, M).$$

Obviant la prova de l'existència d'aquest morfisme, si que cal notar que estem invertint l'ordre de la aplicació, ja que els fixos per G estarán inclosos en els fixos per H, el qual ens rememora a la correspondència de Galois. També podem definir una aplicació similar per al pas al quocient. Si partim de $\pi : G \to G/H$, podem aplicar el mateix pas. Aquí sí que requerim quelcom sobre els mòduls, i és que la acció del quocient estigui ben definida sobre el mòdul, i per tant usarem el mòdul M^H. La aplicació s'anomenarà inflació.

$$\mathrm{Inf} : H^r(G/H, M^H) \to H^r(G, M).$$

Ara podem veure quin tipus de functors son els grups de cohomologia quan actuen sobre la successió curta de grups $1 \to H \to G \to G/H \to 1$, usant aquestes aplicacions que hem definit.

Teorema 3.1. Sigui $H \trianglelefteq G$ i M un G-mòdul. La següent successió és exacta.

$$0 \to H^1(G/H, M^H) \xrightarrow{\mathrm{Inf}} H^1(G, M) \xrightarrow{\mathrm{Res}} H^1(H, M).$$

Anomenarem a aquesta successió, restricció-inflació.

1. L'aplicació inflació és injectiva. Sigui $\phi \in H^1(G/H, M^H)$ amb $\mathrm{Inf}(\phi) = 0$; aleshores $\mathrm{Inf}(\phi)$ és una covora: $\mathrm{Inf}(\phi)(g) = \frac{{}^g m}{m}$ per algun $m \in M$. Però com que prové d'una aplicació a G/H, en qualsevol element $h \in H$, $\mathrm{Inf}(\phi)(gh) = \mathrm{Inf}(\phi)(hg)$ o idènticament $\frac{{}^g m}{m} = \frac{{}^{gh} m}{m}$, per tant ${}^h m = m$. Això implica que $m \in M^H$, amb el qual ϕ també serà una covora a $H^1(G/H, M^H)$.
2. $\mathrm{Res} \circ \mathrm{Inf} = 0$. Si $\phi \in H^1(G/H, M^H)$, aquesta aplicació serà trivial sobre H. Però precisament l'aplicació Res és la restricció sobre H.
3. El nucli de la restricció és $H^1(G/H, M^H)$, o el que és lo mateix, les aplicacions a $H^1(G, M)$ que són trivials sobre H.

Proposició 3.3. Sigui $g_1, \ldots, g_n$ un conjunt de representants de les classes mòdul H. L'aplicació que envia ψ a $\sum_{i=1}^n g_i \psi(g_i^{-1})$ és un morfisme entre $\mathrm{Ind}_H^G(M)$ i M.

A partir d'aquesta aplicació i el lema de Shapiro podem definir la aplicació correstricció com:

$$\mathrm{Cor} : H^r(H, M) \xrightarrow{\mathrm{Shapiro}} H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(G, M)$$

Corol·lari 3.3. Sigui $H \subset G$ un subgrup d'index finit. Aleshores $\mathrm{Cor} \circ \mathrm{Res}(m) = [G : H]m$

Demostració. Si és la multiplicació per l'index a nivell de mòduls, també ho serà a nivell de grups de cohomologia. Prenem $m \in M$ i l'enviem a la aplicació $\psi_m(g) = gm$. Així, al aplicar la correstricció tindrem:

$$\sum_{i=1}^n g_i \psi_m(g_i^{-1}) = \sum_{i=1}^n m = m[G : H].$$

□

Definició 3.9. La component p-primària d'un grup abelià és el subgrup dels elements que s'anul·len al multiplicar per una potència de p.

Corol·lari 3.4. Sigui G un grup finit amb p dividint l'ordre i G_p un p-Sylow. Per qualsevol G-mòdul M, l'aplicació restricció

$$\mathrm{Res} : H^r(G, M) \to H^r(G_p, M)$$

és injectiva sobre la component p-primària de $H^r(G, M)$.

Demostració. Usant el corol·lari anterior i que l'índex $[G : G_p]$ no és divisible per p, es veu que els elements p-primàris no trivials no poden anar a la unitat al multiplicar per un nombre que no divideix p. □

3.5 Productes cup

Sembla força intuitiu fer actuar el grup G sobre productes tensorials de mòduls. És a dir, G actuant sobre $M \otimes N$ de la forma $g(m \otimes n) = gm \otimes gn$.
Recordem que quan parlem de productes tensorials $M \otimes N$ estem parlant d'un mòdul definit com l'únic que transforma en lineal qualsevol aplicació bilineal de $M \times N$ en un altre mòdul P. És a dir, el producte tensorial transforma qualsevol aplicació bilineal $f : M \times N \to P$, amb P un grup abelià, en una única aplicació lineal $\overline{f} : M \otimes N \to G$. complint que si $\otimes$ és el la aplicació que va de $M \times N$ a $M \otimes N$ aleshores es dóna la relació

$$\overline{f} \circ \otimes = f.$$

Un bon exemple de pensar el producte tensorial, en aquest cas de k-mòduls on k és un cos, és $k[X, Y] = k[X] \otimes k[Y]$.
Així, tindrem un equivalent a aquest producte tensorial, ara per a aplicacions d'un grup en un mòdul. Siguin $\phi, \phi' \in \mathrm{Hom}(G, \bigotimes_{i=1}^{r} M_i), \mathrm{Hom}(G, \bigotimes_{i=1}^{s} N_i)$. Definim $\phi \cup \phi'$ com el seu producte cup,

$$\phi \cup \phi'(g) = \phi(g) \otimes \phi'(g).$$

Això també ho podem introduir a la cohomologia usada, i a més indueix una estructura d'àlgebra dins els grups de cohomologia, ja que la cohomologia r-èssima i la s-èssima passaran a la $r + s$-èssima com veiem en el següent teorema.

Teorema 3.2. Sigui G un grup i M, N dos G-mòduls. El producte cup indueix una aplicació

$$H^r(G, M) \otimes H^s(G, N) \to H^{r+s}(G, M \otimes N),$$

amb $(\phi, \phi') \to \phi \cup \phi'$.

Aquest teorema no el demostrarem, però si que podem veure algunes aplicacions senzilles, com per exemple que tenim un morfisme directe entre els elements fixos per G.

$$M^G \otimes N^G \to (M \otimes N)^G$$

Algunes propietats del producte cup que posteriorment necessitarem són les següents.

1. $(\phi \cup \psi) \cup \chi = \phi \cup (\psi \cup \chi)$.
2. $\phi \cup \psi = (-1)^{rs} \psi \cup \phi$.
3. $\mathrm{Res}(\phi \cup \psi) = \mathrm{Res}(\phi) \cup \mathrm{Res}(\psi)$.
4. $\mathrm{Cor}(\phi \cup \mathrm{Res}(\psi)) = \mathrm{Cor}(\phi) \cup \psi$.

3.6 Homologia

De forma complementària al concepte de cohomologia, s'acostuma definir també el d'homologia[7]. El procediment de cara a la definició serà semblant, però requerirem algunes eines addicionals.

Definició 3.10. Sigui G un grup i M un G-mòdul. Definim I_G com el subgrup de $\mathbb{Z}[G]$ tal que la següent successió és exacta:

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

En particular, el podem definir formalment com $I_G = \{g - 1 \mid g \in G\}$. Això també ens permet definir $M_G = M/I_G M$, que seria l'anàleg a M^G; en aquest cas, es tracta del quocient de M més gran que fa que l'acció sigui trivial.

En aquest punt, procedim de forma anàloga a com ho vam fer en la definició de cohomologia. És a dir, definim els functors i els mòduls adequats per desenvolupar la teoria.

Definició 3.11. Direm que un mòdul P és projectiu si $\mathrm{Hom}(P, \cdot)$ és un functor exacte. Identicament, una resolució projectiva serà qualsevol successió exacta que inclogui els mòduls projectus dins d'un mòdul donat M

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \to^{d_0} M \to 0.$$

Fem servir la definició del submòdul M_G com a noció dual del submòdul fix, i l'apliquem a la resolució

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \to 0.$$

Això finalment ens permet definir la noció d'homologia com

$$H_r(G, M) = \frac{\mathrm{Ker}(d_r)}{\mathrm{Im}(d_{r+1})}.$$

De manera anàloga que en el cas de la cohomologia, podem donar interpretacions directes dels primers grups. Per exemple, prenem $H_0(G, M)$ i la successió següent esdevé exacta:

$$(P_1)_G \xrightarrow{d_1} (P_0)_G \xrightarrow{d_0} M_G \to 0.$$

Per tant $H_0(G, M) = M_G$. També podem aplicar el procediment per a obtenir una successió llarga en homologia a la successió exacta curta que defineix I_G.

$$\cdots \to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0.$$

Sabem que $\mathbb{Z}[G]$ és un mòdul projectiu, i per tant $H_r(G, \mathbb{Z}[G]) = 0$ per a qualsevol $r \geq 0$. També podem deduir que $(I_G)_G = I_G/I_G^2$. Amb això obtenim

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to 0.$$

Lema 3.7. Sigui G^{ab} el quocient abelià més gran de G (és a dir, el quocient pel subgrup generat pels commutadors), $G^{\mathrm{ab}} = G/[G, G]$. Aleshores, $G^{\mathrm{ab}} \cong I_G/I_G^2$ i per tant $G^{\mathrm{ab}} \cong H_1(G, \mathbb{Z})$.

Demostració. Prenem l'aplicació $I_G \to G/[G, G]$ que envia $\sigma - 1$ a la classe de σ. És un morfisme i en el seu nucli conté I_G^2 ja que

$$(\tau - 1)(\sigma - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1) \iff \sigma\tau\sigma^{-1}\tau^{-1}[G, G] = [G, G]. \quad \square$$

Per tant, tenim $H_1(G, Z) \cong G^{\mathrm{ab}}$. $\square$

[7]El desenvolupament d'aquestes tècniques està fortament motivat per la topologia algebraica, on juguen un paper clau

3.7 Grups de Tate

Ara agruparem l'homologia i la cohomologia. Primer generalitzarem la idea que ja tenim de normes sobre extensions de cossos a qualsevol mòdul. Fins aquí, podríem haver suposat que G era un grup infinit. Per introduir l'aplicació norma requerirem que el grup sigui finit.

Definició 3.12. La aplicació norma sobre un G-mòdul, amb G-finit $\mathrm{Nm}_G : M \to M$ vé definida per $\mathrm{Nm}_G(m) = \sum_{g\in G} gm$.

Veiem dues propietats senzilles d'aquesta aplicació.

Proposició 3.4. 1. $\mathrm{Im}(\mathrm{Nm}_G) \subset M^G$

2. $I_G M \subset \mathrm{Ker}(\mathrm{Nm}_G)$

Demostració. Recordem que per tot $g \in G$, $gG = G$. Aleshores $g\,\mathrm{Nm}_G(m) = \mathrm{Nm}_G(gm) = \mathrm{Nm}_G(m)$. Per tant, les imatges de la aplicació norma queden fixes per G. Idènticament, $(g-1)\,\mathrm{Nm} = 0$ que demostra la segona part. □

Amb aquests resultats podem veure que l'aplicació norma va de M_G a M^G per a qualsevol G-mòdul. Per tant, tenim un morfisme entre el final de l'homologia i el principi de la cohomologia de la forma:

$$\mathrm{Nm}_G : H_0(G, M) \to H^0(G, M)$$

Per tant, aquest morfisme actuarà com a conector entre ambdós conceptes. Així, donada una successió exacta curta de G-mòduls

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

tindrem una successió exacta llarga entre la homologia i la cohomologia que ens permet definir la noció de grup de Tate.

Definició 3.13. Definim com a grup de Tate r-èssim.

$$H^r_T(G, M) = \begin{cases} H^r(G, M) & r > 0 \\ M^G/\mathrm{Nm}_G(M) & r = 0 \\ \mathrm{Ker}(\mathrm{Nm}_G)/I_G M & r = -1 \\ H_{-r-1}(G, M) & r < -1. \end{cases}$$

Es pot veure que fa exacta la successió llarga

$$\cdots \to H^r_T(G, M_1) \to H^r_T(G, M_2) \to H^r_T(G, M_3) \to H^{r+1}_T(G, M_1) \to \ldots$$

La majoria de resultats que hem vist per a la cohomologia també valen per a aquests grups. Cal observar que per als valors 0 i -1 estem aplicant la cohomologia de manera directa sobre la aplicació norma definida sobre M^G i M_G.
Com que quan apliquem tota aquesta colla de resultats a la teoria de cossos de classes ens farà falta veure com actuen certs grups sobre $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}/\mathbb{Z}$, pensant en una acció trivial d'un grup finit en ells. Veiem els següents resultats sobre els grups de Tate.

Proposició 3.5. Sigui G un grup finit.

1. $H^r_T(G, \mathbb{Q}) = 0$ per tota r.
2. $H^0_T(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ i $H^1_T(G, \mathbb{Z}) = 0$.
3. $\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^2_T(G, \mathbb{Z})$

Demostració. 1. Sigui $m = |G|$. Tenim un isomorfisme a $\mathbb{Q}$ que és la multiplicació per m. Podem transformarlo en un isomorfisme entre els grups de Tate $H^r_T(G, \mathbb{Q})$. Alhora, multiplicar per m és el mateix que multiplicar per 0, ja que és l'ordre del grup. Per tant, l'aplicació seria un isomorfisme i l'aplicació zero, i per tant els grups serán 0.

2. Per a la segona part, com que G actúa trivialment tenim $\mathbb{Z}^G = \mathbb{Z}$ i la norma en aquest cas serà multiplicar per m. També haviem vist anteriorment que, en el cas que l'acció sigui trivial, $H^1(G, M) = \mathrm{Hom}(G, M)$, per tant n'hi ha prou amb agafar un morfisme i veure que és 0. Sigui ϕ un morfisme i $g \in G$. Llavors, tenim que
$$0 = \phi(e) = \phi(g^m) = m\phi(g)$$
però $\mathbb{Z}$ no té torsió per tant $\phi(g) = 0$.

3. Finalment partim de la successió:
$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$
Sabem que ens proporciona una successió més llarga en la cohomología on un tros és:
$$H^1(G, \mathbb{Q}) \to H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Q})$$
Com que els dos extrems són 0, tornant a aplicar $H^1(G, M) = \mathrm{Hom}(G, M)$, ja tenim el resultat.

□

També ens caldrà relacionar els diferents grups de cohomologia de Tate per poder inferir resultats senzills de les cohomologies coneixent només H^0_T, H^1_T, H^2_T.

Proposició 3.6. Sigui G un grup finit cíclic i M un G-mòdul, aleshores $H^r_T(G, M) \cong H^{r+2}_T(G, M)$ per tota r.

No demostrarem aquest ultim resultat però sí que es vol destacar quelcom que és de força rellevància. Es pot escollir canònicament un element $\gamma \in H^2_T(G, \mathbb{Z})$ tal que aquest isomorfisme vingui definit pel producte cup per aquest element. El que nosaltres agafarem serà aquell (recordant que $H^2_T(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$) que enviï un generador del grup ciclic a l'element $\frac{1}{m}$. Retornarem més tard a aquesta precisió.
Partint de que coneixem el significat directe dels grups H^0 i H^1 podem definir relacions entre ells que ens permetin treure conclusions directes quan volguem mirar quina forma tenen sober mòduls concrets.

Definició 3.14. Definim com el quocient de Herbrand la relació $h(M) = \frac{|H^0_T(G,M)|}{|H^1_T(G,M)|}$.

Usant l'hexàgon exacte es veu que partint d'una successió
$$0 \to A \to B \to C \to 0,$$
i suposant que el quocient estigui ben definit, és a dir, que els cardinals són finits, es dóna la relació $h(B) = h(A)h(C)$.

Lema 3.8. Sigui M un G-mòdul finitament generat, aleshores el quocient de Herbrand val $h(M) = 1$.

3.8 El teorema de Tate

Presentem ara un dels resultats més important de cara a establir els teoremes principals de la teoria de cossos de classe. La importància del següent teorema recau sobre un fet que ja hem mencionat anteriorment: la rellevància de l'el·lecció del generador de H^2. Ara no suposarem que el nostre grup sigui cíclic, però sí que imposarem certes condicions sobre els subgrups de G, que podrem controlar ja que G seguirà sent finit.

Teorema 3.3. Suposem que G és finit i que M és un G-mòdul. També imposem les següents condicions sobre els subgrups H:

1. $H^1_T(H, M) = 0$;
2. $H^2_T(H, M)$ és cíclic d'ordre $|H|$.

Aleshores, per tot $r \in \mathbb{Z}$ tenim un isomorfisme
$$H^r_T(G, \mathbb{Z}) \to H^{r+2}_T(G, M)$$
que només depèn de l'elecció del generador de $H^2_T(G, M)$.

Demostració. Brown, LCFT, 4.38 □

4 Teoria local de cossos de classe

Recordem quin és l'objectiu de la teoria de cossos de classe: demostrar que tota la informació sobre les extensions abelianes d'un cos està ja continguda en la propia aritmètica del cos. En altres paraules, els grups de Galois d'aquestes extensions estan relacionats a través d'un morfisme de grups amb el grup $K^\times$, i en particular amb l'extensió abeliana maximal.

4.1 La llei de reciprocitat d'Artin local

Amb l'objectiu de simplificar la notació, obviarem la valoració no-arquimediana, i denotarem per K el nostre cos base local. L'enunciat següent s'anomena llei de reciprocitat local o aplicació d'Artin local i resumeix aquesta idea per a cossos locals (al cap sempre tindrem $\mathbb{Q}_p$):

Teorema 4.1. Sigui K un cos local no-arquimedià (respecte una valoració v). Hi ha un únic morfisme de grups:

$$\phi_K : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

complint les següents propietats:

1. Cada uniformitzador ω de K actúa en el grup de Galois de l'extensió no ramificada maximal com el Frobenius sobre la part no ramificada, és a dir $\phi_K(\omega)|_{K^{nr}} = \mathrm{Frob}_K$.
2. Per tota extensió abeliana L/K finita, l'aplicació esdevé un isomorfisme de grups a través de la norma $\mathrm{Nm}(L^\times)$, és a dir,
$$\phi_{L/K} : K^\times/\mathrm{Nm}(L^\times) \to \mathrm{Gal}(L/K)$$

La demostració d'aquest resultat fa servir totes les eines desenvolupades en les seccions anteriors. Com ja hem apuntat, la clau estarà en trobar un element privilegiat que ens permeti definir l'aplicació. A partir d'això només caldrà relacionar els diferents grups de cohomologia amb els grups que tenim implicats en la llei de reciprocitat.
El primer objectiu serà demostrar que els grups de Tate de L (prenent tots els subgrups del grup de Galois) són cíclics (segona hipòtesi del teorema de Tate). Usant les relacions de restricció i inflació veurem que és suficient provar que $H^2(G, L^\times)$ és cíclic d'ordre el grau de l'extensió. Fixarem això com el primer objectiu d'aquesta secció.
Anem a establir la notació: L/K serà una extensió abeliana de cossos locals amb G el seu grup de Galois. $\mathcal{O}_L$ serà l'anell d'enters de l'extensió (tindrem al cap que $\mathbb{Q}_p$ és el cos de fraccions de $\mathbb{Z}_p$). l i k seràn els respectius cossos residuals (si cal $\mathfrak{m}_L$ i $\mathfrak{m}_K$ seran els ideals maximals). Tots aquests seràn G-mòduls amb l'acció de Galois, i especialment, ho seràn també els seus grups multiplicatius.

Teorema 4.2. (*classe fonamental*) Sigui L/K una extensió de cossos locals de grau n. Llavors, $H^2_T(G, L^\times)$ és un grup cíclic d'ordre n.

A partir d'aqui usarem una sèrie de resultats que fan servir tot el que hem mencionat de cohomologia per demostrar el teorema anterior.

Lema 4.1. Sigui L/K una extensió no ramificada finita. Aleshores,

$$H^r_T(G, l) = H^r_T(G, l^\times) = H^r_T(G, \mathcal{O}_L^\times) = 0$$

per a tot $r \in \mathbb{Z}$.

Demostració. Les notacions indiquen el cos residual l amb la suma i el producte respectivament. Com que estem parlant d'un grup cíclic, en tenim prou amb veure que $H^1_T(G, l) = H^0_T(G, l) = 0$. Recordem que en el cas no ramificat tenim $G = \mathrm{Gal}(l/k)$ i G ha de ser un grup cíclic (extensió finita de cossos finits).
Per al cas additiu, si $r > 0$ ja havíem vist en un dels exemples que la cohomologia d'una extensió finita ha de ser 0. Com que G és cíclic, podem aplicar el resultat d'isomorfisme entre els valors de r de la mateixa paritat per obtenir el resultat per tot r.
Per al cas multiplicatiu, en $H^1_T(G, l^\times)$ tenim el teorema 90 de Hilbert, i en el cas $H^0_T(G, l^\times)$ fem servir que $l^\times$ és un mòdul finitament generat, i per tant, usant el lema 3.8, el quocient de Herbrand val 1, amb el qual

$H^0_T(G, l^\times) = 0$. Aplicant de nou el fet que G és cíclic, obtenim el resultat.
En el cas de $\mathcal{O}_L^\times$, l'exhaustivitat de la norma no és a priori trivial, però també ens permet obtenir $H^r_T(G, \mathcal{O}_L) = 0$. Pel teorema 90 de Hilbert, tenim $H^1_T(G, L^\times) = 0$ i recordant que $L^\times \cong \mathcal{O}_L^\times \times \mathbb{Z}$, només depenent de l'elecció de l'uniformitzador, obtenim també $H^r_T(G, \mathcal{O}_L) = 0$. Ara podem tornar a aplicar de nou que G és cíclic i acabar la prova del teorema. □

Més encara, podem assegurar aquest resultat per a extensions infinites sempre que $r > 0$, passant del limit projectiu que defineix el grup profinit als grups de cohomologia.
Escrivim ara la següent successió exacta, que és només una altra manera d'escriure $L^\times = \mathcal{O}_L \times \mathbb{Z}$.

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{\mathrm{ord}_L} \mathbb{Z} \to 0.$$

Els resultats anterior per $r = 2$ ens donen un isomofrisme $H^2_T(G, L^\times) = H^2_T(G, \mathbb{Z})$. Usant l'isomorfisme definit en la Proposició 3.5 veiem que tenim la següent successió:

$$H^2_T(G, L^\times) \cong H^2_T(G, \mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{av}_{\mathrm{Frob}_L}} \mathbb{Q}/\mathbb{Z}.$$

Al avaluar en el Frobenius (que té ordre n, el grau de l'extensió), ens assegurem que en tots els elements $f \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ satisfan

$$n\,\mathrm{av}_{\mathrm{Frob}_L}(f) = f(\mathrm{Frob}_L^n) = f(1) = 1.$$

Per tant $f(\mathrm{Frob}_L) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. A aquesta aplicació li direm mapa invariant i el notarem per inv_L. En particular, en el cas d'una extensió no ramificada, el Frobenius continua sent el mateix, i per tant, l'ultim morfisme corresponent a avaluar en el Frobenius seria un isomorfisme amb $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

$$H^2_T(G, L^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

Amb això tenim que $H^2_T(G, L^\times)$ és cíclica de grau n, en el cas d'una extensió no ramificada finita.

Proposició 4.1. Sigui L/K una extensió finita de grau n. Si definim $H^2_T(G, L^\times)_{\mathrm{nr}} = H^2_T(G, L^\times) \cap H^2_T(G, K^{\mathrm{nr}\,\times})$, aleshores aquest és un grup cíclic generat per un element $u_L \in H^2_T(G, K^{nr\times})$ amb $\mathrm{inv}_L(u_L) = \frac{1}{n}$.

Demostració. Farem un esquema de la demostració. Partim de la següent successió:

$$0 \to H^2_T(G, L^\times)_{\mathrm{nr}} \to H^2_T(G, K^{\mathrm{nr}\,\times}) \xrightarrow{\mathrm{Res}} H^2_T(G, L^{\mathrm{nr}\,\times}),$$

es veu la commutativitat del següent esquema:

$$\begin{array}{ccc} H^2_T(G, K^{nr\times}) & \xrightarrow{\mathrm{Res}} & H^2_T(G, L^{nr\times}) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

□

Proposició 4.2. Per a tota extensió finita L/K tenim que per algun $U \subset \mathcal{O}_L^\times$ estable sota l'acció de Galois, $H^r_T(G, U) = 0$ per a tot $r \in \mathbb{Z}$.

Per a demostrar la proposició, provarem primer el següent lema.

Lema 4.2. L'aplicació e^x és un isomorfisme entre $\mathfrak{m}_L^n$ amb la suma i $1 + \mathfrak{m}_L^n$ amb el producte sempre que $n > \frac{e}{p-1}$.

Demostració. Hem de comprovar una llista de propietats.

1. L'aplicació és un morfisme ja que $e^{x+y} = e^x e^y$ sobre $\mathfrak{m}_L^n$ i vé donat per la serie $\sum_{n=0}^\infty \frac{x^n}{n!}$.
2. La seva inversa $\ln(x)$ també és un morfisme ja que $\ln(xy) = \ln(x) + \ln(y)$ definit sobre $1 + \mathfrak{m}_L^n$.

3. A nivell formal una és la inversa de l'altre igual que a $\mathbb{R}$, però no és trivial la convergència per elements del nostre cos.

4. Podem demostrar que la convergència d'una sèrie usant la propietat no-arquimediàna de la valoració es dóna si els coeficients tendeixen a zero. *Koblitz, p-adic NAF, 2.* Aleshores

$$\lim_{k\to\infty} v(\frac{x^k}{k!}) = \lim_{k\to\infty} kv(x) - v(k!).$$

Determinem quant val $v(k!)$ de la forma següent: primer mirem elements que tinguin valoració com a mínim 1. Si estiguessim a $\mathbb{Q}_p$ n'hi hauria com a mínim $\frac{k}{p}$, i en el cas d'una altra extensió local, a sobre cal multiplicar per l'índex de ramificació ja que les valoracions dels elements del cos base queden multiplicades per aquest element. Seguim aquest procés buscant quants elements tenen valoració com a mínim m, i seran com a molt $\frac{ek}{p^m}$. Per tant, comptem en una valoració cadascun d'aquests nombres i obtenim la fita superior

$$ke\sum_{j=1}^{\infty}\frac{1}{p^j} = \frac{ke}{p}\frac{1}{1-\frac{1}{p}} = \frac{ke}{p-1}.$$

Per tant, trobem la fita inferior:

$$\lim_{k\to\infty} k(v(x) - \frac{e}{p-1}),$$

i si el nombre de dins del parèntesi és positiu convergirà a ∞ que és la valoració que volem, és a dir, la del 0. Per acabar només cal notar que si $x \in \mathfrak{m}_L^n$, aleshores $v(x) > n$.

□

Demostració. (*de la proposició*) El teorema de la base normal ens dóna una base $\{x_\sigma \mid \sigma \in G\}$ de l'extensió. Podem prendre $d \in \mathcal{O}_L$ tal que $dx_\sigma \in \mathcal{O}_L$ sigui una base amb elements enters. Sigui $U = \sum \mathcal{O}_L x_\sigma$. En particular $U = \mathcal{O}_L[G] = \mathrm{Ind}_1^G(\mathcal{O}_L)$. Aplicant el lema de Shapiro a tots els grups de Tate,

$$H_T^r(G,U) = H_T^r(1,\mathcal{O}_L) = 0.$$

Ara hem de transferir això al grup multiplicatiu. Ho fem a partir de l'isomorfisme definit en el lema anterior. Aquest isomorfisme estarà enviant entorns oberts del 0 a entorns oberts de l'1. Per tant, per qualsevol obert V, podem agafar $\omega^N V$ un entorn del zero de manera que l'isomorfisme l'envii a un obert U complint que $H_T^r(G,U) = 0$, i també és $H_T^r(G,\omega^M V) = 0$ per tot $r \in \mathbb{Z}$. □

Proposició 4.3. Per a tota extensió L/K cíclica de grau n, $h(\mathcal{O}_L^\times) = 1$ i $h(L^\times) = n$. En particular, $H_T^2(G, L^\times)$ té ordre n.

Demostració. Prenem U el subgrup obert de $\mathcal{O}_L^\times$ que té els grups de Tate nuls i apliquem la multiplicativitat del quocient de Herbrand: $h(\mathcal{O}_L^\times) = h(\mathcal{O}_L^\times/U)h(U)$. Ambdós factors valen 1: el primer per ser quocient d'un compacte per un obert, ha de ser finit i per tant té cohomología nula, i el segon pels resultats anteriors. Per tant, $h(\mathcal{O}_L^\times) = 1$.
En el cas de $L^\times$ ja hem usat diverses vegades que $L^\times = \mathcal{O}_L^\times \times \mathbb{Z}$. Tornem a usar la multiplicativitat per obtenir que $h(L^\times) = h(\mathbb{Z})$. Per calcular aquest últim quocient de Herbrand sabem que $|H_T^0(G,\mathbb{Z})| = n$ i $|H_T^1(G,\mathbb{Z})| = 1$.
Usant el 90 de Hilbert, $H_T^1(G,L^\times) = 0$ i per tant $|H_T^0(G,L^\times)| = n$. A partir de la periodicitat, sabem que $H_T^2(G,L^\times)$ té el mateix ordre. □

Lema 4.3. Sigui G un grup finit i M un G-mòdul. Siguin $q, r > 0$ enters. Suposem que:

1. $H_T^i(H,M) = 0$ per a $0 < i < r$ i tots els subgrups H de G;

2. si $H \subset K \subset G$, amb H normal a K i K/H cíclic d'ordre primer, aleshores $H_T^r(H,M)$ divideix $[K:H]^q$.

Aleshores es compleix el mateix per a G, és a dir, l'ordre de $H_T^r(G,M)$ divideix $|G|^q$

Demostració. El primer que volem veure és que podem suposar que G és un p-grup. En cas contrari, podem prendre G_p un p-Sylow i veure que la aplicació restricció Res : $H^r_T(G,M) \to H^r_T(G_p,M)$ és injectiva en els punts del domini que tenen p^∞-torsió, és a dir, els que tenen ordre alguna potència de p. Per tant, si $|H^r_T(G_p,M)|$ divideix $|G_p|$, també $|H^r_T(G,M)|$ divideix $|G|$. Ho provem per inducció sobre l'ordre de G.
Per $r>0$, prenem H un subgrup d'índex p i apliquem la inducció usant la successió de restricció-inflació

$$0 \to H^r_T(G/H, M^H) \xrightarrow{\text{Inf}} H^r_T(G,M) \xrightarrow{\text{Res}} H^r_T(H,M)$$

En el cas trivial de l'ordre de G, tot és trivial ja que tota la cohomologia també és trivial. Per les hipòtesis suposades i la inducció tenim que $H^r_T(H,M)$ divideix $|H|^q$ i també que $H^r_T(G/H,M^H)$ divideix p^q. Usant que la successió és exacta, es demostra que

$$|H^r_T(G,M)| \;\Big|\; |H^r_T(H,M)||H^r_T(G/H,M^H)| \;\Big|\; [G:H]^q|H|^q = |G|^q$$

Per $r=0$ no tenim la cadena de restricció-inflació però si que tenim la següent successió exacta

$$M^H/\operatorname{Nm}_H(M) \xrightarrow{\text{Nm}_{G/H}} M^G/\operatorname{Nm}_G(M) \xrightarrow{id_G} (M^H)^{G/H}/\operatorname{Nm}_{G/H}(M^H)$$

a la qual podem aplicar el mateix argument que abans. Per veure que la successió és exacta pensar que els elements del nucli de la identitat són els que tenen norma que queda fixa per H, equivalents als de la primera part. □

Teorema 4.3. Sigui L/K una extensió finita de grau n. Llavors $H^2_T(G,L^\times)$ és cíclic d'ordre n, generat per un element $u_L \in H^2_T(G,L^{\text{nr}})$ complint $\text{inv}_L(u_L) = \frac{1}{n}$. Més específicament, escriurem $u_{L/K}$ quan partim d'un cos K i una extensió L/K.

Demostració. Apliquem el resultat anterior a $M = L^\times$, $q=1$ i $r=2$. La primera hipòtesi vé donada pel teorema 90 de Hilbert en un cert subgrup. La segona pel corol·lari anterior prenent un grup cíclic que el contingui. Per tant, l'ordre de $H^2_T(G,L^\times)$ també divideix n si l'extensió no és necessàriament cíclica. Però ja teniem que conté alguna extensió cíclica, en particular $H^2_T(G,(L^{\text{nr}})^\times)$. Així $H^r_T(G,L^\times)$ també serà cíclic generat pel mateix element. En particular, $H^2_T(G,\overline{K}) = H^2_T(G,K^{\text{nr}})$. □

Teorema 4.4. Sigui L/K una extensió de Galois finita. Aleshores, el producte cup $\alpha \to \alpha \cup u_L$ defineix un isomorfisme entre $H^r_T(G,\mathbb{Z})$ i $H^{r+2}_T(G,L^\times)$

Demostració. Aplicació del teorema de Tate. La primera hipòtesi és el teorema 90 de Hilbert. La segona és aplicació del teorema anterior. Amb això ja estem en condicions d'enunciar el resultat sobre el mapa de reciprocitat local. □

Teorema 4.5. Sigui L/K una extensió abeliana finita. Tenim un isomorfisme entre entre $\text{Gal}(L/K)$ i $K^\times/\operatorname{Nm}(L^\times)$.

Demostració. N'hi ha prou amb prendre en el teorema anterior $r=-2$. Tindrem:

$$K^\times/\operatorname{Nm}(L^\times) \cong H^0_T(G,L^\times) \cong H^{-2}_T(G,\mathbb{Z}) \cong H_1(G,\mathbb{Z}) \cong \text{Gal}(L/K)$$

Aquest ultim isomorfisme apareix al lema 3.5, i que el grup de Galois és abelià. □

4.2 Comportament de la aplicació d'Artin per torres

Donada una torre d'extensions $K \subset E \subset L$, volem provar que la aplicació d'Artin que hem definit és la mateixa si prenem qualsevol subextensió.

Proposició 4.4. En la torre anterior,

$$\phi_L(x)|_E = \phi_E(x)$$

per a tot $x \in K$.

Lema 4.4. Usant les aplicacions de restricció sobre $H^2(G,L^\times)$ obtenim

1. $\mathrm{Res}(u_{L/K}) = u_{L/E}$
2. $\mathrm{Inf}(u_{E/K}) = [L:E]u_{L/K}$

Demostració. La prova es fa aplicant el lema nucli-conucli a les files del següent diagrama

$$\begin{array}{ccccc} H^2_T(\overline{K}/K) & \xrightarrow{\mathrm{Res}} & H^2_T(\overline{K}/E) & \xrightarrow{\mathrm{Res}} & H^2_T(\overline{K}/K) \\ \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_E} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[E_K]} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$

on els H^2_T són els grups de Tate amb l'acció del corresponent grup de Galois de cada extensió. Amb això obtenim un nou diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2_T(E/K) & \xrightarrow{\mathrm{Inf}} & H^2_T(L/K) & \xrightarrow{\mathrm{Res}} & H^2_T(L/E) \\ & & \downarrow{\scriptstyle \mathrm{inv}_{E/K}} & & \downarrow & & \downarrow{\scriptstyle \mathrm{inv}_{L/E}} \\ 0 & \longrightarrow & \frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} & \xrightarrow{[L_K]} & \frac{1}{[L:E]}\mathbb{Z}/\mathbb{Z} \end{array}$$

on els grups G són els corresponents grups de Galois. Es pot demostrar que és commutatiu i a partir d'això es veuen els resultats.
A partir de la commutativitat d'aquests dos diagrames, es demostra que les aplicacions restricció i correstricció es comporten com volem per al producte cup.

$$\mathrm{Res}(u_{L/K} \cup \beta) = u_{L/E} \cup \mathrm{Res}(\beta)$$

$$\mathrm{Cor}(u_{L/E} \cup \beta) = u_{L/K} \cup \mathrm{Cor}(\beta)$$

□

L'aplicació d'Artin serà la mateixa en els dos casos, el qual equival a la proposició anterior. Això ens permetrà que l'aplicació d'Artin inicial estigui definida com $phi_K : K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ i compleixi la segona propietat del teorema inicial.

4.3 La imatge de l'endomorfisme de Frobenius

Per acabar de demostrar el teorema inicial ens fa falta veure també el comportament dels uniformitzadors.

Proposició 4.5. Sigui L/K una extensió no ramificada i G el seu grup de Galois. L'element $\mathrm{Frob}_{L/K}$ va a la classe d'ω, un uniformitzador sota l'aplicació d'Artin. Equivalentment, $\phi_{L/K}(x) = \mathrm{Frob}_{L/K}^{\mathrm{ord}_p(x)}$.

Per exemple, prenem $\mathbb{Q}_p$ i una extensió ramificada seva L. El seu grup de Galois equival al grup de Galois d'una extensió finita de cossos finits, generada pel Frobenius. El primer p seria un uniformitzador, i qualsevol element $x \in K$ s'escriu com $x = up^r$. Si la proposició anterior és certa tenim la imatge d'aquest element seria $\phi_L(x) = \mathrm{Frob}^r_{L/K}$.

Definició 4.1. Sigui $u_L \in H^2_T(G, L^\times)$ el representant canònic que genera el grup de Tate, usant $\phi : G^2 \to M$ com a cocicle representant. Aleshores $M(\phi)$ és la suma directa $M \oplus Z$ on Z és el grup lliure generat per els símbols x_σ amb $\sigma \in G$. L'acció de G sobre $M(\phi)$ és:

$$\sigma(m, x_\tau) = (\sigma m + \phi(\sigma, \tau), x_{\sigma\tau} - x_\sigma)$$

La prova de la proposició consisteix a veure que l'element de Frobenius va a un uniformitzador ω via l'aplicació d'Artin. Amb la següent demostració, reseguirem el camí que fa ω a través de l'aplicació canònica definida per el teorema de Tate.

Demostració. Prenent el mòdul $L^\times(\phi)$ i el $\mathbb{Z}[G]$ tenim les següents seqüències exactes. La primera ja l'hem vista, la segona és la descomposició[8] del mòdul que hem definit.

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0,$$

$$0 \to L^\times \to L^\times(\phi) \to I_G \to 0.$$

Es pot veure que els grups de Tate d'ambdós mòduls $L^\times(\phi)$ i $\mathbb{Z}[G]$ són nuls i per tant tenim isomorfismes

$$H_T^{-2}(G,\mathbb{Z}) \to H_T^{-1}(G,I_G)$$

$$H_T^{-1}(G,I_G) \to H_T^0(G,L^\times).$$

En el primer cas ja vem estudiar l'isomorfisme al lema 3.5, i vem veure que $\sigma = \mathrm{Frob}_{L/K} \in G^{\mathrm{ab}}$ es mou a l'element $\sigma - 1 + I_G^2$ a I_G/I_G^2. El que cal veure és on va aquest últim element en el segon isomorfisme. Per això, usarem el lema de la serp mitjançant el següent diagrama que connecta H_T^{-1} i H_T^0.

$$\begin{array}{ccccccc} & & & & & & H_T^{-1}(G,I_G) \\ & & & & & & \downarrow \\ 0 & \longrightarrow & (L^\times)^G & \longrightarrow & (L^\times(\phi))^G & \longrightarrow & (I_G)^G \\ & & \downarrow & & & & \\ & & H_T^0(G,L^\times) & & & & \end{array}$$

L'aplicació entre $L^\times(\phi)$ i I_G envia (m,x_σ) a $\sigma - 1$. Per tant, hem de computar la norma de $(1,x_\sigma)$ que és una antiimatge de $\sigma - 1 + I_G^2$.

$$\mathrm{Nm}_G(1,x_\sigma) = \sum_{i=1}^{n-1} \sigma^i(1,x_\sigma) = \sum_{i=1}^{n-1} (\phi(\sigma,\sigma^i), x_{\sigma^{i+1}} - x_{\sigma^i}) = (\prod_{i=1}^{n-1} \phi(\sigma,\sigma^i), 1).$$

Per acabar la demostració per a un uniformitzador ω cal veure que

$$\phi(\sigma^i,\sigma^j) = \begin{cases} 1 & \text{si } i+j \leq n-1 \\ \omega & \text{si } i+j < n-1. \end{cases}$$

Això últim és un càlcul fet amb eines semblants a la construcció de la classe fonamental, recordant que en el mapa invariant enviem l'element σ^i a $\frac{i}{n} \in \mathbb{Q}/\mathbb{Z}$.
Finalment com que ja sabiem que $H_T^0(G,\mathcal{O}_L^\times) = 0$, aleshores $\mathcal{O}_K^\times = (\mathcal{O}_L^\times)^G = \mathrm{Nm}_G(\mathcal{O}_L^\times) \subset \mathrm{Nm}_G(L^\times)$ el qual vol dir que $\omega = u\omega$ a $K^\times/\mathrm{Nm}_G(L^\times)$ per a qualsevol unitat $u \in \mathcal{O}_K^\times$. □

4.4 Subgrups de norma

El propòsit de la teoria de cossos de classe és classificar totes les extensions abelianes només en funció d'informació continguda al cos base. Per tant, un cop construida l'aplicació d'Artin, volem veure com es condensa aquesta informació dins el nostre cos local a través dels subgrups $\mathrm{Nm}(L)$. Per tant, hem de veure quins subgrups de $K^\times$ són normes d'alguna extensió.

Proposició 4.6. Sigui $N \subset K^\times$. N és un de la forma $\mathrm{Nm}(L)$ per alguna extensió L/K, si i només si, N és obert d'index finit.

Pensem en el cas del cos $\mathbb{Q}_p$:

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z} = \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}$$

Es pot provar que en cossos de característica 0 (els p-àdics ho són), tots els subgrups d'index finit són oberts. Per tant, hem d'estudiar els subgrups d'index finit de cadascun dels factors.

[8] Aquesta descomposició es computa exactament igual ja que $L^\times(\phi) = L^\times \oplus I_G$

1. A $\mathbb{Z}/(p-1)\mathbb{Z}$ tots els seus subgrups tenen índex finit i els tenim classificats per tots els divisors de $p-1$.

2. A $\mathbb{Z}$ tots els seus subgrups tenen índex finit són els $n\mathbb{Z}$.

3. A $\mathbb{Z}_p$ hem de prendre subgrups U_n dels $\mathbb{Z}/p^n\mathbb{Z}$ i prendre'n el limit projectiu $U = \varprojlim U_n$

Com que no tenen ordres coprimers entre si necessàriament, podem trobar altres subgrups que provinguin de barrejar elements de les diferents parts.
Per demostrar el resultat, ens cal usar els desenvolupaments de Lubin-Tate i els grups formals, eines que també s'apliquen enaltres branques de la teoria de nombres. Prendrem K un cos local, $\mathcal{O}_K$ el seu anell d'enters, ω un uniformitzador de K i k el seu cos residual amb q elements.

Definició 4.2. Una serie de potències formal ω-àdica és una sèrie de potències a $\mathcal{O}_K[[X]]$ tal que:

1. $f(X) = \omega X \mod X^2$.

2. $f(X) = X^q \mod \omega$.

Denotem per $\mathcal{F}_\omega$ aquest conjunt.

Exemple 4.1. Si $K = \mathbb{Q}_p$, la sèrie $F(X) = pX + \binom{p}{2}X^2 + \dots pX^{p-1} + X^p = (X+1)^p - 1$ és d'aquesta forma.

Definició 4.3. Una llei de grup formal commutativa sobre un anell A és una sèrie de potencies $F \in A[X,Y]$ complint:

1. $F(X, F(Y,Z)) = F(F(X,Y), Z)$.

2. $F(0,Y) = Y$ i $F(X,0) = X$.

3. Existeix una única $G(X)$ amb $F(X, G(X)) = 0$.

4. $F(X,Y) = F(Y,X)$.

5. $F(X,Y) = X + Y \mod$ grau 2.

Definició 4.4. Un morfisme entre dues lleis de grup F, G és una sèrie de potències en dues variables tal que:

$$h(F(X,Y)) = G(h(X), h(Y))$$

Proposició 4.7. Per tota $f \in \mathcal{F}_\omega$, existeix una llei de grup formal commutativa F_f amb coeficients a $\mathcal{O}_K$ que fa f un endomorfisme de la llei de grup, és a dir:

$$f(F_f(X,Y)) = F_f(f(X), f(Y))$$

Proposició 4.8. Sigui $f \in \mathcal{F}_\omega$ i F_f la llei de grup de la proposició anterior. Aleshores per tot $\alpha \in \mathcal{O}_K$, existeix una sèrie de potències $[\alpha]_f \in \mathcal{O}_K[[X]]$ tal que:

1. $[\alpha]_f$ commuta amb f.

2. $[\alpha]_f = \alpha X \mod$ grau 2.

Així, $[\alpha]_f$ és un endomorfisme de la llei de grup F_f.

Proposició 4.9. Sigui $f, g \in \mathcal{F}_\omega$. Aleshores, $F_f \cong F_g$.

També necessitarem alguna relació entre dos uniformitzadors.

Proposició 4.10. Siguin ω i $u\omega$ a $\mathcal{O}_v$ dos uniformitzadors (u és una unitat) amb F_f, F_g dos grups formals definits a $f \in \mathcal{F}_\omega$ i $g \in \mathcal{F}_{u\omega}$. Aleshores, existeix $\epsilon \in \mathcal{O}_{\hat{K}^{\mathrm{nr}}}^\times$ tal que $\mathrm{Frob}_K(\epsilon) = u\epsilon$ i una sèrie de potències $h(T) \in \mathcal{O}_{\hat{K}^{\mathrm{nr}}}[[T]]$ complint.

1. $h(X) \equiv \epsilon X(\mod$ grau 2).

2. $\text{Frob}_K \circ h = h \circ [u]_f$
3. $h(F_f(X,Y)) = F_g(h(X,h(Y))$.
4. $h \circ [a]_f = [a]_g \circ h$ per tot $a \in \mathcal{O}_K$.

Ens estalviarem les proves d'aquests resultats per evitar enfarfegar el treball amb massa contingut, no necessàriament relacionat amb el treball. Els desenvolupaments dels grups formals i els seus morfismes són mètodes generals i també podrien aplicarse a altres branques de la teoria de nombres. En aquest cas els usarem per demostrar quins són els subgrups de norma. El següent pas és demostrar que la extensió totalment ramificada maximal de K, que denotarem K^{tr}, és la que es construeix afegint la torsió del grup formal corresponent a un uniformitzador (en el cas de $\mathbb{Q}_p$, totes les arrels d'ordre una potència de p).
Prenem $f \in \mathcal{F}_\omega$ i F_f la llei de grup corresponent. Definim com M_f el grup de punts de $\mathfrak{m}_{\overline{K}}$ l'ideal maximal d'una clausura algebraica de K equipats amb la llei de grup F_f. Prenem E_f^n els nuclis dels endomorfismes $[\omega^n]_f$. Si un x pertany a E_f^n, això implica $\omega^n x = 0$ mòdul grau 2, és a dir, que és un punt d'ω^n-torsió en M_f.
Així podem prendre les extensions $K^n = K(E_f^n)$ i $K_\omega = \cup_{n\geq 1} K^n$ i $G_{\omega,n} = \text{Gal}(K^n/K)$ els seus grups de Galois amb $\text{Gal}((K_\omega/K) = \varprojlim G_{\omega,n}$.

Proposició 4.11. Considerant E_f^n com un mòdul amb l'acció de $\mathcal{O}_K$, obtenim

1. $\text{End}_{\mathcal{O}_K}(E_f^n) \cong \mathcal{O}_K/(\omega^n)$.
2. $\text{Aut}_{\mathcal{O}_K}(E_f^n) \cong (\mathcal{O}_K/(\omega^n))^\times$.

Demostració. Demostrarem que $E_f^n \cong \mathcal{O}_K/(\omega)$. Un cop haguem vist això, tant el grup additiu com el grup multiplicatiu de $\mathcal{O}_K$ donen lloc a una acció sobre el conjunt E_f^n. Sabem que qualsevol acció d'un grup ens dóna un morfisme de grups entre el grup i les permutacions del conjunt que en el cas additiu serà:

$$\mathcal{O}_K \to \text{End}_{\mathcal{O}_K}(E_f^n).$$

En aquest cas, el morfisme serà exhaustiu i el nucli ho formaran els morfismes que representin la identitat que seran els que enviïn cada element de torsió al 0, és a dir els de la forma $k\omega^n$, per tant el nucli serà el que volem. En el segon cas valdrà el mateix per a l'acció del grup multiplicatiu.
Per inducció sobre n, demostrarem el primer isomorfisme. Usant la proposició 4.9, es veu que és indiferent el f que estiguem prenent. En el cas de $n = 1$ tenim $[\omega]_f = \omega \cdot X + X^q$. Si prenem qualsevol element $x \in \mathfrak{m}_{\overline{K}}$, $f(X) - x$ té alguna arrel en la clausura algebraica. Usant un procediment anomenat "polígons de Newton" *Milne, ANT, 7.44*, veiem que totes les seves arrels cauen dins de $\mathfrak{m}_{\overline{K}}$. Prenem totes les arrels de f i corresponen al nucli de $[p]_f$, per tant aquest equival a E_f^1. Com que és un endomorfisme, podem aplicar el teorema d'isomorfisme canviant el nucli per la imatge, quan sabem que la imatge sempre serà l'ideal generat per ω.
El pas inductiu el veiem a través de la successió exacta:

$$0 \to E_f^1 \to E_f^n \xrightarrow{[p]_f} E_f^{n-1} \to 0.$$

□

Exemple 4.2. Per a $\mathbb{Q}_p$, podem prendre un isomorfisme de E_p^n i les arrels p^n-èssimes de la unitat. Tot i això, la relació no és directa sinó que ho és a través del canvi de variable $y = x + 1$. Sigui y una arrel p-èssima de la unitat. Aleshores es compleix que:

$$1 = (x+1)^p = \sum_{i=0}^{p} \binom{p}{i} x^i.$$

Per tant x és arrel de $F(X) = \sum_{i=1}^{p} \binom{p}{i} X^i$ que pertany a $\mathcal{F}_p$. Per a exponents majors també es pot veure. Moralment, quan afegim els conjunts E_f^n estem afegint les arrels p^n-èssimes de la unitat.

Lema 4.5. Sigui L/K una extensió de Galois. Per qualsevol $f \in \mathcal{O}_K[[X]]$ i $x \in \mathfrak{m}_L$.

$$f(\sigma(x)) = \sigma(f(x))$$

per tot $\sigma \in \text{Gal}(L/K)$.

Demostració. En cas que $f(\sigma(x))$, el resultat és trivial. L'únic que hem de veure és que si x convergeix, aleshores $\sigma(x)$ també. Això es veu, un cop sabem que $x \in \mathfrak{m}_L^n$ per algun n, aleshores $\sigma(x)$ també, i per tant usant els arguments del lema 4.2, també convergirà. □

Teorema 4.6. Amb la notació usada fins ara tenim els següents resultats.

1. K^n/K és una extensió totalment ramificada de grau $(q-1)q^{n-1}$.
2. Tenim un isomorfisme entre $(\mathcal{O}_K/(\omega^n))^\times \simeq G_{\omega,n}$.
3. ω és una norma en K_ω.

Per a que sigui més visual dibuixem l'esquema, on a cada pas estem afegint la torsió del grup formal, que en el cas de $\mathbb{Q}_p$, coincideix amb afegir les arrels q-èssimes de la unitat.

$$\begin{array}{c} K_\omega \\ \cdots \\ \Big| q \\ K^2 \\ \Big| q \\ K^1 \\ \Big| q-1 \\ K \end{array}$$

Demostració. Prenem x_1 una arrel de $f(X)$ diferent de zero. El seu polinomi mínim és $X^{q-1}+\omega$ que és ω-Eisenstein, per tant l'extensió $K(x_1)/K$ és totalment ramificada i té grau $q-1$.
Així podem anar construint la torre d'extensions Eisenstein afegint, en el pas n-èssim, una arrel del polinomi $f(X)-x_{n-1}$ que serà x_{n-1}-Eisenstein, prenent x_i com el nou uniformitzador a cada pas[9]. Tindrem les extensions $K(x_1,\dots,x_n)/K(x_1,\dots,x_{n-1})$ que tenen grau q.
Aquests elements compliran que $f(x_1)=0$ i $f^n(x_n)=f^{n-1}(f(x_n))=f^{n-1}(x_{n-1})=\cdots=f(x_1)=0$. Així pensem ara $G_{\omega,n}=\mathrm{Gal}(K^n/K)$ com un subgrup del simètric sobre E_f^n i per tant com un subgrup de $Aut(E_f^n)=(\mathcal{O}_K/(\omega^n))^\times$ que té $(q-1)q^{n-1}$ elements [10]. Amb això podem veure que $K(x_1,\dots,x_n)=K^n$ veient que tenen el mateix grau

$$(q-1)q^{n-1}=[K(x_1,\dots,x_n):K]\leq[K^n:K]=|\,\mathrm{Gal}(K^n/K)|\leq(q-1)q^{n-1}$$

Aquesta ultima igualtat demostra la segona part del teorema. Ara provem que els elements x_n que hem près tenen norma ω. Primer vegem que el seu polinomi mínim és $h_n=g\circ f^{n-1}$ on $g(X)=X^{q-1}+\omega$ complint $h_n(x_n)=h_{n_1}(x_{n-1})=\cdots=g(x_1)=0$. Té grau el producte de tots els graus de la composició que és $(q-1)q^{n-1}$ i per tant ha de ser el mínim. Sabent això

$$\mathrm{Nm}_{K^n/K}(x_n)=(-1)^{(q-1)q^{n-2}}\omega$$

que val q quan $n\geq 1$. □

Prenent el limits projectius obtendriem

$$\mathcal{O}_K^\times=\varprojlim(\mathcal{O}_K/(\omega^n))^\times=\varprojlim\mathrm{Gal}(K^n/K)=\mathrm{Gal}(K_{v,\omega}/K).$$

Amb això ja tenim descrita l'extensió totalment ramificada maximal de K que denotarem per K^{tr}. K^{nr} serà la no ramificada maximal i clarament $K^{\mathrm{nr}}\cap K^{\mathrm{tr}}=K$. Definim la aplicació següent

$$\phi_\omega : K^\times \to \mathrm{Gal}(K^{\mathrm{tr}}K^{\mathrm{nr}}/K^r)$$

[9] Un element que generi una extensió totalment ramificada serà un uniformitzador.
[10] com a anell té p^n elements dels quals p^{n-1} són invertibles

definida sobre cada element per restricció sobre cadascuna de les extensions. Ho farem de la següent manera sobre $a \in K^\times$ de la forma $a = u\omega^n$

$$\phi_\omega(a)\big|_{K^{\mathrm{nr}}} = \mathrm{Frob}_K^n \quad \phi_\omega(a)\big|_{K^{\mathrm{tr}}} = [u^{-1}]_f.$$

El que volem demostrar és que aquesta aplicació coincideix amb la nostra aplicació d'Artin i en particular que $K^{\mathrm{tr}}K^{\mathrm{nr}} = K^{\mathrm{ab}}$. Endemés, que no depèn de l'uniformitzador que agafem.

Lema 4.6. Sigui L/K una extensió algebraica i $\hat{L}$ la compleció de L respecte la valoració induïda. Prenem $x \in \hat{L}$. Si x és separable i algebraic, aleshores $x \in L$.

Demostració. Prenem $L' = \hat{L} \cap \overline{K}$. Prenem $\sigma \in \mathrm{Gal}(\overline{K}/L)$ i veurem que fixa també L', el qual usant teoria de Galois ens donarà el resultat desitjat. Sigui $x \in L'$, que al ser de la compleció de L serà limit de elements $x_i \in L$. Per tant, $\sigma(x_i) = x_i$ i $\sigma(x)$ serà limit d'aquests elements i per ser una extensió algebraica i separable, σ serà contínua i com a tal, $\sigma(x) = x$. □

Teorema 4.7. El cos $K^{\mathrm{tr}}K^{\mathrm{nr}}$ és independent de l'elecció de l'uniformitzador, així com l'aplicació ϕ_p.

Demostració. Prenem ω i π dos uniformitzadors que es diferencien d'una unitat u, $f \in \mathcal{F}_\omega$ i $g \in \mathcal{F}_\pi$ i h com definida en la proposició 4.10. Volem relacionar les arrels de f amb les de g.

$$\mathrm{Frob}_{K_v} \circ h \circ [\omega]_f = h \circ [u]_f \circ [\omega]_f = h \circ [\pi]_f = [\pi]_g \circ h.$$

Això ens dóna $h(f(T))^q = g(h(T))$, per tant si $f(\alpha) = 0$ aleshores $g(h(\alpha)) = 0$ [11]. També si $g(\beta) = 0$ implica $f(h^{-1}(\beta)) = 0$. Per tant, h defineix una bijecció entre les arrels de f (E_f^1) i g (E_g^1). Amb això

$$\hat{K}_v^{\mathrm{nr}}(E_g^1) = \hat{K}_V^{\mathrm{nr}}(h(E_f^1)) \subset \hat{K}_v^{\mathrm{nr}}(E_f^1) = \hat{K}_v^{\mathrm{nr}}(h^{-1}(E_g^1)) \subset \hat{K}_v^{\mathrm{nr}}(E_g^1).$$

Usant el lema anterior podem treure la condició de completesa i obtenim $K^{nr}(E_g^1) = K^{nr}(E_f^1)$. Un argument molt semblant usant $[\omega^n]_{f,g}$ val per les arrels E_f^n.
Ara veiem que la aplicació no depèn de l'uniformitzador. En la part no ramificada, el valor de n no canvia si variem l'uniformitzador. Només falta veure-ho per $K_{v,\omega}$. Siguin ω, π els dos uniformitzadors anteriors. És obvi que $\phi_\omega(\omega)$ és la identitat. Volem veure que $\phi_\pi(\omega)$ també és la identitat. És suficient demostrar-ho per $x \in K^n$ per qualsevol n. Per tant, prenem h la bijecció anterior i volem veure que

$$\phi_\pi(\omega)(h(x)) = h(x)$$

o equivalentment, $\phi_\pi(\omega) = \phi_\pi(u^{-1})\phi_\pi(\pi) = \tau_1\tau_2$.

$$\phi_\pi(\omega)(h(x)) = \tau_1\tau_2(h(x)) =_{\text{Lema 4.5}} \tau_1(h(\tau_2(x))) =_{\text{Prop 4.10}} \tau_1(h([u]_f(x))) = h(x).$$

□

Proposició 4.12. Per tota $n, m \in \mathbb{Z}$ es té

$$\phi_\omega(x)\big|_{K^n K_m} = \mathrm{id}$$

per tot $x \in (1 + \mathfrak{m}_v^n)(\omega^m)$ on K_m és la única extensió no ramificada de grau m, donada per l'extensió dels cossos residuals de grau m.

Demostració. Tenim $x = up^{m'}$ amb $m' \geq m$ i $u \in (1+\mathfrak{m}_v^n)$. Prenem $y \in K_m$, aleshores i $\overline{y}$ el seu representant a k_m el cos residual.

$$\overline{\phi_\omega(x)(y)} = \mathrm{Frob}_K^{m'}(\overline{y}) = \overline{y}$$

com que l'extensió té inèrcia trivial aquest element de Galois també fixarà y.
Per l'altra part, $y' \in K^n$ que podem suposar que és un element de E_f^n. Apliquem ϕ_ω sobre x i tenim

$$\phi_\omega(x)(y') = [u]_f(y') = y'.$$

□

[11] Usant que h no té terme constant pel punt 1 de la proposició 4.10.

Corol·lari 4.1. Per tot $x \in K^\times$, $\phi_K(x)\big|_{K_\omega K^{nr}} = \phi_\omega(x)$.

Demostració. Per tot n, ω és una norma a K^n com hem vist en el teorema 4.6. Per tant, $\phi_K(\omega)$ és trivial sobre K^n amb el qual $\phi_\omega(a)\big|_{K^n} = \phi_{K^n}$. En el teorema anterior, prenent $m = 1$ també és veu que $\phi_\omega(\omega)$ és trivial. Endemés, en la part no ramificada, les imatges de l'uniformitzador actuen com el Frobenius en els dos casos. Les aplicacions coincideixen per la unió $\cup_{n\geq 1} K^n K^{\mathrm{nr}} = K^{\mathrm{tr}} K^{\mathrm{nr}}$. □

Lema 4.7. Per tota $n, m \geq 0$ sigui $K^{n,m} = K^n K_m$. Aleshores, $\mathrm{Nm}((K^{n,m})^\times) = (1 + \mathfrak{m}_v^n)(\omega^m)$.

Demostració. La proposició 4.12 i el lema 4.8 ens diuen que si $x \in (1 + \mathfrak{m}_v^n)(\omega^m)$, aleshores $\phi_{K}\big|_{K^{n,m}}$ actúa trivialment i $x \in \mathrm{Nm}((K^{n,m})^\times)$. L'altra inclusió la veiem a través l'equivalencia entre els graus

$$[K^\times : (1 + \mathfrak{m}_v^n)(\omega^m)] = [\mathcal{O}_K^\times : 1 + \mathfrak{m}_v^n][(\omega) : (\omega^m)] = (q-1)q^n m = [K^n : K][K_m : K] = [K^{n,m} : K]$$

Per tant tenim un isomorfisme de grups

$$\phi_{K^{n,m}} : K^\times / \mathrm{Nm}((K^{n,m})^\times) \to \mathrm{Gal}(K^{n,m}/K)$$

i per tant $\mathrm{Nm}((K^{n,m})^\times) = (1 + \mathfrak{m}_v^n)(\omega^m)$. □

Al final d'aquest capítol, es poden trobar exemples d'aquests subgrups per a $\mathbb{Q}_p$.

Lema 4.8. Sigui L/K una extensió finita i $\mathrm{Nm}(L^\times)$ d'índex finit. Aleshores $\mathrm{Nm}(L^\times)$ és obert a $K^\times$.

Demostració. Per la proposició 2.2, $\mathcal{O}_L$ és compacte. i per tant tancat. Com que els unics elements que tenen norma unitat són les unitats, podem construir la inclusió

$$\mathcal{O}_K^\times / \mathrm{Nm}(\mathcal{O}_L^\times) \hookrightarrow K^\times / \mathrm{Nm}(L^\times).$$

En les valoracions discretes, els tancats d'index finit són oberts i $\mathrm{Nm}(\mathcal{O}_L^\times)$ ho és. $\mathrm{Nm}(L^\times)$ conté un obert d'index finit, per definició d'obert també ho serà. □

Teorema 4.8. $\phi_K = \phi_\omega$ i $K^{\mathrm{ab}} = K^{\mathrm{nr}} K^{\mathrm{tr}}$.

Demostració. Sigui L/K una extensió abeliana finita. Sabem que $K^\times / \mathrm{Nm}(L^\times) \cong \mathrm{Gal}(L/K)$, per tant $\mathrm{Nm}(L^\times)$ és d'índex finit i pel lema anterior també és obert. Per tant, haurà de contenir algun $(1 + \mathfrak{m}_K^n)(\omega^m)$, amb el qual $L \subset K^{n,m}$. També tenim que el mapa d'Artin sobre $LK^{n,m} = K^{n,m}$ és exhaustiu i que $\phi_K(x)$ fixa els elements de L, si i nomes si, pertany a $\mathrm{Nm}(L^\times)$. Si prenem el limit per totes les n, m obtindrem l'extensió $K_{v,\omega} K^{\mathrm{nr}}$ i també unint totes les extensions abelianes obtenim K^{ab}. Això també implica $\phi_\omega = \phi_K$. □

Teorema 4.9. Sigui $N \subset \mathbb{Q}_p^\times$ un subgrup. N és de la forma $\mathrm{Nm}(L^\times)$ per alguna extensió finita abeliana, si i només si, N és d'index finit i obert.

Demostració. Ja sabem que els subgrups de norma són d'índex finit perquè els quocients estan en bijecció amb grups de Galois d'extensions finites. Usant el lema 4.8 també són oberts. Prenem ara $N \subset K^\times$ d'índex finit i obert. Per la demostració del lema 4.7, sabem que existeixen n, m tals que $\mathrm{Nm}(K^{n,m}) = (1 + \mathfrak{m}_v^n)(\omega^m) \subset N$. Per tant, prenem L com el subcos de $K^{n,m}$ fix per $\phi_{K^{n,m}/K}(N)$. D'aquí treiem que N és el nucli de $\phi_K : K^\times \to \mathrm{Gal}(L/K)$, per tant $N = \mathrm{Nm}(L^\times)$. □

Ja tenim caracteritzades totes les extensions abelianes de K. En particular, tenim quina és l'extensió ciclotòmica maximal. Sabem que en qualsevol cas, aquesta extensió és el resultat de afegir la ω^n-torsió del grup formal, que en el cas de $\mathbb{Q}_p$ són les arrels p^n-èssimes de la unitat, amb el qual $K^{\mathrm{ab}} = K^{\mathrm{cicl}}$. Això és el teorema de Kroenecker-Weber en la seva versió local. De fet, podem trobar una analogia en el mètode usat aquí i en la primera secció, ja que en ambdós casos hem afegit aquestes arrels.

El següent teorema demostra que el que hem fet no val per a les extensions no abelianes, és a dir que mantindriem el mateix subgrup de norma, i per tant, no tindriem una bijecció entre subgrups de norma i extensions qualsevols.

Teorema 4.10. (*de limitació de la norma*) Sigui E una extensió de $\mathbb{Q}_p$ qualsevol i L l'extensió abeliana més gran continguda a E. Aleshores

$$\mathrm{Nm}(E^\times) = \mathrm{Nm}(L^\times).$$

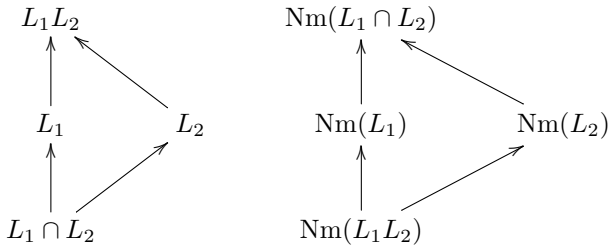
Demostració. Usant les propietats de la norma $\mathrm{Nm}_{E/K} = \mathrm{Nm}_{E/L} \circ \mathrm{Nm}_{L/K}$, veiem que $\mathrm{Nm}_{E/K}(E^\times) \subset \mathrm{Nm}_{L/K}(L^\times)$. També tenim que el grup de Galois abelià més gran dins de $\mathrm{Gal}(E/K)$ és $\mathrm{Gal}(L/K)$.

$$K/\mathrm{Nm}(L^\times) \cong \mathrm{Gal}(L/K) \cong \mathrm{Gal}(E/K)^{\mathrm{ab}} \cong K/\mathrm{Nm}(E^\times).$$

Fent servir la inclusió, ens dóna la igualtat. □

També podem caracteritzar la bijecció que hem construit entre les extensions a través d'un reticle de la forma següent.

Teorema 4.11. Tenim un diagrama de la forma



Per veure l'equivalència entre aquests diagrames cal demostrar les següents propuetats:

1. $L_1 \subset L_2$, si i només si, $\mathrm{Nm}_{L_1/K}(L_1^\times) \supset \mathrm{Nm}_{L_2/K}(L_2^\times)$.
2. $\mathrm{Nm}_{L_1L_2/K}((L_1L_2)^\times) = \mathrm{Nm}_{L_1/K}(L_1^\times) \cap \mathrm{Nm}_{L_2/K}(L_2^\times)$.
3. $\mathrm{Nm}_{(L_1\cap L_2)/K}((L_1 \cap L_2)^\times) = \mathrm{Nm}_{L_1/K}(L_1^\times)\,\mathrm{Nm}_{L_2/K}(L_2^\times)$.

Demostració. Una implicació de (1) ja l'hem vista en l'anterior teorema. L'altra implicació es veu comprovant que l'aplicació que envia L a $\mathrm{Nm}\, L/K(L^\times)$ és bijectiva.
Amb (1) també veiem que $\mathrm{Nm}_{L_1L_2/K}((L_1L_2)^\times) \subset \mathrm{Nm}_{L_1/K}(L_1^\times) \cap \mathrm{Nm}_{L_2/K}(L_2^\times)$. Altrament, prenem $a \in \mathrm{Nm}_{L_1/K}(L_1^\times) \cap \mathrm{Nm}_{L_2/K}(L_2^\times)$ i aleshores $\phi_{L_1/K}(a) = \phi_{L_1/K}(a) = 1$. A més, l'aplicació restricció de $\mathrm{Gal}(L_1L_2/K)$ a cadascún dels grups de Galois és injectiva. D'aqui treiem $\phi_{L_1L_2/K}(a) = 1$ i amb això ja tenim (2).
Per veure l'últim, n'hi ha prou amb pensar que $L_1 \cap L_2$ és la subextensió més gran que està en ambdues L_1 i L_2; i $\mathrm{Nm}_{(L_1\cap L_2)/K}((L_1 \cap L_2)^\times)$ és el subgrup més petit que conté ambdós $\mathrm{Nm}_{L_1/K}(L_1^\times)$ i $\mathrm{Nm}_{L_2/K}(L_2^\times)$. Un cop sabem això, podem fer servir la bijecció per obtenir el resultat desitjat. □

4.5 Exemples de cossos de classe locals quadràtics

Recuperem ara la secció del capítol 2 on parlavem de les extensions quadràtiques de $\mathbb{Q}_p$. Hem vist que per $p > 2$ tenim tres extensions quadràtiques, de les quals només una és no ramificada. D'acord amb el desenvolupament teòric que hem fet en aquesta secció, hauríem de trobar 3 subgrups de $\mathbb{Q}_p^\times$ que tinguin índex 2.
Per fer això descomponem $\mathbb{Q}_p^\times$.

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p^\times \cong \mathbb{Z} \times 1 + p\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$$

Cada tros de la descomposició té un subgrup d'índex 2.

1. El primer és $2\mathbb{Z} \times 1 + p\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$. Com que l'uniformitzador p no serà trivial quan fem quocient per aquest subgrup, i va a l'element de Frobenius en el cos de classe corresponent, aquest cos ha de ser l'extensió no ramificada. En el cas de $p = 5$, és $\mathbb{Q}_5(\sqrt{2})$.

2. El segon subgrup és $\mathbb{Z} \times 1 + p\mathbb{Z}_p \times U$ on U és un subgrup cíclic d'ordre $\frac{p-1}{2}$, de manera que en aquest es correspon amb afegir una arrel del propi uniformitzador, per tant, quan $p = 5$, correspon al subgrup $\mathbb{Q}_5(\sqrt{5})$.

3. L'últim subgrup correspon als elements de la mateixa paritat a $\mathbb{Z}$ i $\mathbb{Z}/(p-1)\mathbb{Z}$. Per exemple, els elements $(1,1),(2,2),\ldots,(p-1,0),\ldots$. En el nostre exemple correspon al cos de classes $\mathbb{Q}(\sqrt{10})$.

En el cas de $p = 2$, tenim la descomposició

$$\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \times 1 + 4\mathbb{Z}_2$$

i hem de trobar 7 subgrups, tres d'ells són els subgrups d'ordre dos en cada factor de la descomposició.

1. L'extensió no ramificada s'associa al subgrup $2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \times 1 + 4\mathbb{Z}_2$, i correspon a $\mathbb{Q}_2(\sqrt{2})$.

2. Per a la resta d'extensions, partim de les dues extensions disjuntes $\mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{3})$ que corresponen als subgrups d'ordre 2 obtinguts a partir de cada factor de la descomposició $\mathbb{Z}/2\mathbb{Z}$ i $1 + 4\mathbb{Z}_2$. Les que falten les podem construir a partir d'aquestes.

5 Teoria global de cossos de classe

L'objectiu d'aquesta secció és obtenir els resultats clàssics de la teoria de cossos de classe. Als apartats anteriors, ens hem servit de les propietats algebraiques i topològiques dels cossos locals, com la seva topologia o el fet que només tenen un ideal primer. Ara, ens proposem a pensar els mateixos resultats per a cossos de nombres, és a dir, extensions finites de $\mathbb{Q}$, per tant, el primer que volem veure és com es pot sintetitzar la informació dels seus ideals primers, en termes dels valors absoluts.
Sigui K un cos de nombres. Definirem com una plaça una classe d'equivalència de valors absoluts en aquest cos. Tenim tres tipus de classes d'equivalència:

1. Direm que una plaça és finita si prové d'un valoració respecte un ideal primer. Per exemple, prenent $p \in \mathbb{Z}$, v_p és d'aquest tipus.

2. Direm que una plaça és infinita real si prové d'una immersió del cos dins $\mathbb{R}$. Per exemple, el valor absolut habitual a $\mathbb{Q}$.

3. Direm que una plaça és infinita complexa si prové d'una immersió del cos dins de $\mathbb{C}$. En aquest cas venen en parells d'immersions complexes conjugades. Per exemple, la immersió trivial a $\mathbb{Q}(i)$ i la seva conjugada.

Es pot demostrar un anàleg al teorema d'Ostrowski per a qualsevol cos de nombres, veient que qualsevol valoració no trivial en un cos de nombres provindrà d'alguna d'aquests tres tipus. Direm que un ideal primer pertany a un conjunt de places S si el valor absolut induït per la seva valoració apareix en alguna de les classes d'equivalència de S.

5.1 El grup de classes de S

Definició 5.1. Sigui I_K el conjunt d'ideals fraccionaris de K. Sigui S un conjunt finit de places del cos. Definim, I_K^S com el subgrup de I_K generat pels ideals primers que no estàn a S.

És a dir, tot ideal $\mathfrak{a} \in I_K^S$ s'escriu com $\mathfrak{a} = \mathfrak{p}_1^{n_1}\mathfrak{p}_2^{n_2}\dots\mathfrak{p}_s^{n_s}$ amb $\mathfrak{p}_i \notin S$ i $n_i \in \mathbb{Z}$. També podem identificar-lo amb el grup lliure generat per les places de K que no apareixen a S.

Definició 5.2. Altrament, podem definir dins I_K^S els seus ideals principals com el subgrup

$$K^S = \{\, a \in K^\times \mid (a) \in I_K^S \,\} = \{\, a \in K^\times \mid \mathrm{ord}_\mathfrak{p}(a) = 0 \text{ per tot } \mathfrak{p} \in S \,\}.$$

Exemple 5.1. Sigui $n \in \mathbb{Z}$. Prenem com a S el conjunt de primers que divideixen n. El grup $\mathbb{Q}^S$ són les fraccions $\frac{r}{s}$ tals que $\mathrm{mcd}(s,n) = \mathrm{mcd}(r,n) = 1$.

Lema 5.1. Donat un cos K i un conjunt finit de places S, tenim la successió exacta de grups

$$0 \to \mathcal{O}_K^\times \to K^S \to I_K^S \to C \to 0,$$

on C és el grup de classes.

Demostració. La primera fletxa és una inclusió injectiva. En la segona, l'ideal total pot ser representat per qualsevol unitat. En la tercera, l'element neutre de C és la classe dels ideals fraccionaris principals, és a dir, els (α) amb $\alpha \in K^S$. Prenem ara $\mathfrak{a} \in C$, el qual podem suposar que és enter [12]. Per tant, $\mathfrak{a}$ s'escriu com $\mathfrak{a} = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}$ amb $\mathfrak{b} \in I_K^S$. Per cada $\mathfrak{p} \in S$ prenem $\omega_\mathfrak{p}$ un uniformitzador de la localització en aquest primer. Usant el teorema xinès del residu, existeix $a \in \mathcal{O}_K$ complint

$$a \cong \omega_\mathfrak{p}^{n(\mathfrak{p})} \mod \mathfrak{p}^{n(\mathfrak{p})+1}$$

per cada $\mathfrak{p} \in S$. Amb això tenim que $(a) = \mathfrak{a} = \prod_{\mathfrak{p}\in S}\mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$ amb $\mathfrak{b}' \in I_K^S$. Per tant, $a^{-1}\mathfrak{a} \in I_K^S$ i representa la mateixa classe al grup C. □

[12] En cas contrari, escrivim un ideal qualsevol $\mathfrak{a} = \frac{\mathfrak{b}}{\mathfrak{c}}$ amb $\mathfrak{b}, \mathfrak{c}$ ideals enters, de manera que per tot $c \in \mathfrak{c}$, $\mathfrak{a}(c) = \frac{\mathfrak{b}}{\mathfrak{c}}(c)$ és enter i representa la mateixa classe que $\mathfrak{a}$.

Definició 5.3. Un modulus a K és una aplicació:

$$m : \{ \text{ places de K } \} \to \mathbb{Z}$$

complint les tres condicions següents

1. $m(\mathfrak{p}) = 0$ excepte per un nombre finit de places.
2. $m(\mathfrak{p}) = 0, 1$ si $\mathfrak{p}$ és infinita real.
3. $m(\mathfrak{p}) = 0$ si és infinita complexa.

Podem pensar un modulus com un producte finit de places de la forma.

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$$

Direm que un modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}$ divideix a un altre $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$ si per a tota plaça. $\mathfrak{p}$ $m(\mathfrak{p}) \leq n(\mathfrak{p})$. En particular un primer $\mathfrak{p}$ tal que $m(\mathfrak{p}) > 0$ divideix el modulus $\mathfrak{m}$. Denotarem per $S(\mathfrak{m})$ el conjunt de places que divideixen $\mathfrak{m}$.

Definició 5.4. Sigui $\mathfrak{m}$ un modulus en un cos K, i definim com $K_{\mathfrak{m},1}$ el conjunt dels $a \in K^\times$ que compleixen.

1. $\text{ord}_{\mathfrak{p}}(a-1) \geq m(\mathfrak{p})$ en totes les places que divideixin $\mathfrak{m}$.
2. $|a|_{\mathfrak{p}} > 0$ en les places infinites reals.

Notem si $a \in K_{\mathfrak{m},1}$, $\text{ord}_{\mathfrak{p}}(a-1) > 0 = \text{ord}_{\mathfrak{p}}(1)$.

$$\text{ord}_{\mathfrak{p}}(a) = \text{ord}_{\mathfrak{p}}(a-1+1) = \min(\text{ord}_{\mathfrak{p}}(a-1), \text{ord}_{\mathfrak{p}}(1)) = 0$$

Llavors a no pertany a cap dels ideals que divideixen $\mathfrak{m}$, o el que és el mateix, $(a) \in I_K^{S(\mathfrak{m})}$. Per tant, podem construir l'aplicació

$$i : K_{\mathfrak{m},1} \hookrightarrow I_K^{S(\mathfrak{m})}$$

que envia a, un element del cos, a (a), un ideal fraccionari que no dividirà el modulus.

Amb això podem construir un anàleg al grup de classes però només per a un nombre finit de places. Aquesta construcció ja és representativa de la teoria que volem construir: agafant un nombre de places finit, el nostre cos es podrà pensar com un producte de cossos locals.

Definició 5.5. Definim el grup de classes d'un modulus o grup de classes radial com $C_{K,\mathfrak{m}} = I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$

Aquesta definició transforma la successió de lema 6.1 en una nova successió.

Lema 5.2. Sigui $\mathfrak{m}$ un modulus. Tenim la successió exacta

$$0 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{K,\mathfrak{m}} \to C_K \to 0,$$

on $K_{\mathfrak{m}} = K^{S(\mathfrak{m})} = \{ a \in K^\times \mid \text{ord}_{\mathfrak{p}}(a) = 0 \text{ per } \mathfrak{p} \text{ divideix } \mathfrak{m} \}$, $U = \mathcal{O}_K^\times$ i $U_{\mathfrak{m},1} = U \cap K_{\mathfrak{m},1}$.

Demostració. La primera injecció és trivial donat que si un element és unitat de l'anell d'enters del cos, el seu ordre és 0 en totes les places, per tant $U \subset K_{\mathfrak{m}}$.
La segona aplicació la veiem prenent un element $\overline{x} \in K_{\mathfrak{m}}/K_{\mathfrak{m},1}$ que vagi a la classe trivial al grup $C_{\mathfrak{m}}$. Per tant, també pertany a la classe trivial a $K_{\mathfrak{m}}/K_{\mathfrak{m},1}$, $\overline{x} = \overline{1}$. I aquesta classe és imatge de la classe del 1 a $U/U_{\mathfrak{m},1}$.
Per a la tercera i la quarta hem de considerar la inclusió $i_I : I_K^{S(\mathfrak{m})} \hookrightarrow I_K$, que és exhaustiva i es transforma en una inclusió $i_C : C_{K,\mathfrak{m}} \hookrightarrow C$. □

5.2 Formulació clàssica amb ideals

Tal i com hem vist a la secció 1.3, per a cada extensió L/K i un primer $\mathfrak{p}$ de K no ramificat, tenim un únic element $\sigma = \left(\frac{\mathfrak{p}}{L/K}\right)$, complint les condicions $\sigma(\mathfrak{P}) = \mathfrak{P}$ i $\sigma(x) = x^{N(\mathfrak{p})} \mod \mathfrak{p}$. Això ens permet definir el mapa d'Artin global.

Teorema 5.1. (*Mapa d'Artin global*) Donat un modulus $\mathfrak{m}$, existeix un morfisme

$$\Psi_{L/K} : I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$$

complint que $\Psi_{L/K}(\mathfrak{p}_1^{n_1} \dots \mathfrak{p}_s^{n_s}) = \prod_{i=0}^{s} \left(\frac{\mathfrak{p}_i}{L/K}\right)^{n_i}$.

Demostració. L'existència d'aquesta aplicació és conseqüència de l'existència de l'element de Frobenius quan l'extensió no ramifica. □

Aquesta aplicació, igual que en el cas local, s'estén a través de la norma. Primer hem de definir norma per al cas d'ideals. Com abans, sigui f el grau de l'extensió finita de cossos residuals. La norma d'un ideal a L és

$$\mathrm{Nm}_{L/K}(\mathfrak{P}) = \mathfrak{p}^f.$$

En particular per a $\mathfrak{P} = (\alpha)$, $\mathrm{Nm}_{L/K}((\alpha)) = (\mathrm{Nm}_{L/K}(\alpha))$.

Teorema 5.2. Sigui L/K una extensió abeliana, i K' un cos intermedi. Aleshores el següent diagrama commuta

$$\begin{array}{ccc} I_{K'}^{S(\mathfrak{m})} & \xrightarrow{\Psi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow{\scriptstyle i} \\ I_K^{S(\mathfrak{m})} & \xrightarrow{\Psi_{L/K}} & \mathrm{Gal}(L/K) \end{array}.$$

Amb aquest teorema ens demostra que $\mathrm{Nm}_{L/K}(I_L^S)$ cau dins el nucli del mapa d'Artin, per tant hi haurà una aplicació

$$\Psi_{L/K} : I_K^{S(\mathfrak{m})} / \mathrm{Nm}(I_L^{S(\mathfrak{m})}) \to \mathrm{Gal}(L/K).$$

Però donat que el grup inicial no és necessàriament finit, no tenim de manera trivial un isomorfisme.
El teorema central de la teoria de cossos de classe dóna les condicions per a que la aplicació sigui un isomorfisme.

Teorema 5.3. (*Llei de reciprocitat*) Sigui L/K una extensió abeliana i S el conjunt de primers que ramifiquen en l'extensió. Aleshores existeix un modulus $\mathfrak{m}$ tal que $S = (\mathfrak{m})$, i un isomorfisme definit a partir de l'aplicació d'Artin [13]

$$\hat{\Psi}_{L/K} : I_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}) \,\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})}) \to \mathrm{Gal}(L/K).$$

Als subgrups de la forma $H = i(K_{\mathfrak{m},1}) \,\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})})$, que queden encabits entre els ideals fraccionaris del modulus i els ideals principals els anomenem subgrups de congruència:

$$i(K_{\mathfrak{m},1}) \subset H \subset I_K^{S(\mathfrak{m})}.$$

També val a dir que si un modulus satisfà aquest teorema, tots els que tinguin exponents més grans en els seus primers també valdran.

Definició 5.6. Donat un primer $\mathfrak{p}$ en l'extensió L/K existeix un exponent $\mathfrak{f}(\mathfrak{p})$ tal que en qualsevol altre modulus on s'apliqui el teorema anterior $\mathfrak{f}(\mathfrak{p}) \leq m(\mathfrak{p})$: el modulus $C_{\mathfrak{f}} = \mathfrak{m}_\infty \prod \mathfrak{p}^{\mathfrak{f}(\mathfrak{p})}$. A aquest modulus l'anomenem conductor.

En altres paraules, donada una extensió, construim un modulus i un subgrup de congruencia. Però per a que la construcció valgui en les dues direccions també hem de saber construir una extensió donat un subgrup de congruencia d'un modulus.

[13] Quan ens referim a $(\mathfrak{m})$ ideals en L, ens referim a aquells que estiguin per sobre d'ideals de $S(\mathfrak{m})$ en K

Teorema 5.4. (*Teorema d'existència*) Per cada subgrup de congruència H d'un modulus $\mathfrak{m}$, existeix una extensió abeliana finita L/K tal que $H = i(K_{\mathfrak{m},1})\,\mathrm{Nm}_{L/K}(I_L^{S(\mathfrak{m})})$.

En particular podem prendre el subgrup de congruència mínim $i(K_{\mathfrak{m},1})$ i per tant l'aplicació d'Artin estarà definida sobre el grup de classes radial $C_{K,\mathfrak{m}}$.

Definició 5.7. L'extensió L/K finita abeliana que val per a aquest subgrup s'anomena cos de classes radial. En particular per al modulus $\mathfrak{m} = 1$, l'anomenem cos de classes de Hilbert i coincidirà amb l'extensió no ramificada maximal.

Aquesta notació no és la que usarem per demostrar els resultats, però sí què és més fàcil extreure d'aquí el teorema de Kroenecker-Weber en la seva versió per a cossos de nombres.

Corol·lari 5.1. Siguin L, M dues extensions abelianes de K. Aleshores $L \subset M$, si i només si, existeix un modulus $\mathfrak{m}$, dividit per tots els primers que ramifiquen a M o a L, complint

$$i(K_{\mathfrak{m},1}) \subset \mathrm{Ker}(\Psi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Psi_{L/K,\mathfrak{m}}).$$

Demostració. En una direcció, suposem que $L \subset M$, aleshores l'aplicació restricció funciona a nivell de grups de Galois $r : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$. Per la llei de reciprocitat existirà algun modulus $\mathfrak{m}$ on els dos nuclis $\mathrm{Ker}(\Psi_{L/K,\mathfrak{m}}), \mathrm{Ker}(\Psi_{M/K,\mathfrak{m}})$ són subgrups de congruència. Usant la definició que hem pres d'aplicació d'Artin es pot veure que $\Psi_{L/K} = r \circ \Psi_{M/K}$, amb el qual $\mathrm{Ker}(\Psi_{M/K,\mathfrak{m}}) \subset \mathrm{Ker}(\Psi_{L/K,\mathfrak{m}})$.
En l'altra direcció, podem pensar l'aplicació d'Artin restringida a M: $\Psi_{\mathfrak{m}} \to \mathrm{Gal}(M/K)$. Prenem $H \subset \mathrm{Gal}(M/K)$ la imatge de $\mathrm{Ker}(\Psi_{L/K,\mathfrak{m}})$. Prenem $\hat{L}$ l'extensió dels elements de M fixos per H de manera que $K \subset \hat{L} \subset M$. Això també ens diu que $\mathrm{Ker}(\Psi_{L/K,\mathfrak{m}}) = \mathrm{Ker}(\Psi_{\hat{L}/K,\mathfrak{m}})$. Aleshores, per l'unicitat en el teorema d'existència, $L = \hat{L} \subset M$. □

Exemple 5.2. Prenem $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ l'extensió ciclotòmica m-èssima, i $\mathfrak{m}$ el modulus que conté les places infinites reals i les finites que divideixen m. Aleshores, l'aplicació d'Artin

$$\Psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} : I_{\mathbb{Q}}^{S(\mathfrak{m})} \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}.$$

De fet, podem veure que la imatge d'un ideal $\frac{a}{b}$ que estigui en el modulus (per tant que a, b siguin coprimers amb m) serà la classe de $\frac{[a]}{[b]}$ a $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Amb això veiem que $\frac{a}{b} - 1$ divideix m i per tant el seu ordre en totes les places finites del modulus és positiu, i per suposat en la única plaça infinita és positiu, és a dir $\frac{a}{b} \in i(K_{\mathfrak{m},1})$, que ens diu que $\mathrm{Ker}(\Psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = i(K_{\mathfrak{m},1})$.
Igualment, si ens donen un modulus $\mathfrak{m}$ a $\mathbb{Q}$, l'extensió ciclotòmica m-èssima, on m és el producte de tots els primers que representen les places finites de $\mathfrak{m}$ ens donarà un bon comportament de l'aplicació d'Artin.

Corol·lari 5.2. (Kroenecker-Weber) Tota extensió abeliana de $L/\mathbb{Q}$ està continguda en una extensió ciclotòmica.

Demostració. Per la llei de reciprocitat, existeix un modulus de manera que $i(K_{\mathfrak{m}}, 1) \subset \mathrm{Ker}(\Psi_{L/K})$. Però, com ja hem vist en l'exemple anterior, podem construir un m de manera que l'extensió ciclotòmica m-èssima $\mathbb{Q}(\zeta_m)$ doni $\mathrm{Ker}(\Psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) = i(K_{\mathfrak{m},1}) \subset \mathrm{Ker}(\Psi_{L/\mathbb{Q},\mathfrak{m}})$. □

5.3 Formulació idèlica

No entrarem en les proves clàssiques d'aquests teoremes ja que requereixen nombrosos requisits tècnics basats en les propietats anal·lítiques de les L-sèries. Aquestes proves van ser donades al segle passat per matemàtics com Takagi, Hecke o el mateix Emil Artin *Janusz, ANF, 2.* A més, són anteriors a la idea introduïda per Hasse de recuperar els resultats per a cossos globals les lleis de reciprocitat local. Aquest esquema és el que s'ha seguit en aquesta monografia, però per a que sigui viable demostrar els anteriors resultats per aquest camí s'ha d'indroduir una notació nova.
Un dels problemes amb els quals ens trobem a l'hora de voler estendre les nocions locals és que a prori no tenim cap equivalència topològica entre un cos global i el producte de les seves places. Als capítols anteriors ha passat desaparcebut que al donar un isomorfisme entre $K^{\times}$ i el grup de Galois de l'extensió abeliana maximal, també donavem una relació entre les topologies a ambdós costats: en un cas, la topologia del cos

local, i en l'altre, la topologia de Krull, que en el cas finit és la topologia discreta. Ambdues topologies conservaven la compacitat local, propietat definitòria dels cossos locals.
Per contra, si pretenem escriure un cos global com a producte infinit de les places $K^\times = \prod_v K_v^\times$, perdem aquesta propietat en el producte. Per tant, el primer que necessitem és un espai prou bo en el qual conservar la compacitat local i alhora la idea d'un cos com a producte de les seves places. Començarem per definir un espai topològic prou bo en el qual es mantinguin aquestes propietats.

Lema 5.3. Sigui (X_i) una col·lecció d'espais topològics Hausdorff i localment compactes indexats per un conjunt d'índex arbitràri I. Aleshores, l'espai $X = \prod_{i\in I} X_i$ és localment compacte, si i només si, llevat d'un nombre finit, els espais X_i són compactes.

Demostració. Sabem que la projecció $p_i : X \to X_i$ és continua per tot $i \in I$. Escollim un subconjunt finit $E \subset I$, i per cada $i \in E$, prenem un subconjunt $U_i \subset X_i$. Amb això definim el rectangle

$$R(U_i) = \prod_{i\in E} U_i \times \prod_{i\notin E} X_i$$

que serà obert o tancat, en funció de si ho són els U_i. La topologia producte es defineix com a unions de rectangles oberts. Si l'espai és localment compacte, existiran rectangles oberts que serveixin com a entorn de qualsevol punt, amb adherència compacta. Projectant sobre l'adherència obtindrem que llevat d'un nombre finit, tots els X_i han de ser compactes. En l'altra direcció si que podem aplicar el teorema de Tychonoff que ens diu que el producte de compactes serà compacte. □

Definició 5.8. Sigui X_i una col·lecció d'espais topològics com els del teorema anterior, i K_i una col·lecció de compactes oberts en cada espai topològic. El producte restringit dels X_i respecte K_i es defineix com:

$$\hat{\prod_{i\in I}}^{K_i} X_i = \{(x_i) \in \prod_{i\in I} X_i \mid x_i \in K_i \text{ llevat d'un nombre finit}\}.$$

Servint-nos del lema anterior podem demostrar la compacitat local del producte restringit.

Proposició 5.1. Si els X_i són localment compactes, aleshores el producte restringit $\hat{\prod}_{i\in I} X_i$ és localment compacte.

Demostració. Prenem $x \in \hat{\prod}_{i\in I} X_i$ i E el conjunt finit de x_i que no estàn en K_i. En aquests punts, prenem un entorn compacte U_i. Aleshores, $\prod_{i\in E} U_i \times \prod_{i\notin E} K_i$ és un entorn compacte del punt. □

Passem ara en un cos K i totes les seves valoracions v, anomenant K_v a les completacions respecte aquestes valoracions.

Definició 5.9. L'anell adèlic o adèle d'un cos respecte totes les seves valoracions es defineix com

$$\mathbb{A}_K = \{(x_v) \in \prod_v K_v \mid x_v \in \mathcal{O}_{K_v} \text{ llevat d'un nombre finit}\}.$$

Exemple 5.3. Podem pensar en $\mathbb{Q}$ com el producte restringit de totes les seves places. L'anell adèlic corresponent seria

$$\mathbb{A}_\mathbb{Q} = \hat{\prod}_{p\in S} \mathbb{Q}_p$$

on S és el conjunt de places donades pel teorema d'Ostrowski.

Els anells adèlics dels cossos de nombres mantenen la propietat de compacitat local ja que $\mathbb{Q}_p$ té aquesta propietat. Com que la llei de reciprocitat l'hem definida sobre el grup multiplicatiu de cada cos local, ens interessarà pensar en el grup de les unitats d'aquest anell.

Definició 5.10. El grup d'idèles d'un cos K és el grup de les unitats de l'anell adèlic, o equivalentment

$$\mathbb{I}_K = \{(x_v) \in \prod_v K_v^\times \mid x_v \in \mathcal{O}_{K_v}^\times \text{ llevat d'un nombre finit}\}.$$

La topologia del grup d'idèles sí que compleix aquelles propietats que desitgem. Per exemple una base d'oberts és $\prod_v U_v$ on U_v és un obert de $K_v^\times$ i és $\mathcal{O}_K^\times$ per a quasi bé totes les places. Per determinar $\mathbb{I}_K$ com a grup topològic, donem una base d'entorns de l'element neutre [14] que seria per a cada conjunt S de places:

$$U(S,\epsilon) = \{\, (a_v) \in \mathbb{I}_K \,|\, |a_v - 1|_v < \epsilon,\ v \in S\ |a_v|_v = 1\ v \notin S\}.$$

També hem de construir alguna equivalència entre aquest grup d'idèles i els ideals fraccionaris a través d'un morfisme exhaustiu:

$$i : \mathbb{I}_K \to I_K$$

de manera $\mathrm{id}[(a_v)] = \prod_v p^{\mathrm{ord}_v(a_v)}$ que té per nucli l'idèle de les places infinites.
D'alguna manera, hem de conservar també la idea d'ideals principals. Per fer això, injectem el grup K dins el grup d'idèles a través del morfisme

$$D : K^\times \to \mathbb{I}_K$$

$D(a) = (a, a, \dots)$ en cada plaça. Està ben definit, ja que apareixen un nombre finit de places al descomposar a en factors irreductibles i és injectiu.

Definició 5.11. Definim el grup de classes idèlic com $\mathcal{C}_K = \mathbb{I}_K / D(K^\times)$.

Definició 5.12. Sigui L/K una extensió de cossos de nombres. Siguin w, v places de L, K respectivament. Direm que la plaça w està per sobre de v si la restricció de qualsevol dels valors absoluts de w a K és un valor absolut de v.

A efectes pràctics, en les places finites, direm que w està per sobre de v si l'ideal primer corresponent a w de L divideix a l'ideal primer corresponent a v. En el cas de les places infinites, direm que una plaça per sobre d'una altra si les immersions corresponents estàn contingudes l'una en l'altra.

Definició 5.13. Sigui L/K una extensió de Galois. Definim la norma idèlica de $\mathfrak{I} = (a_w) \in \mathbb{I}_L$ com

$$\mathrm{Nm}_{L/K}(\mathfrak{I}) = ,$$

de manera que en una plaça $\mathfrak{p}$ de K, $b_v = \prod_{w|v} \mathrm{Nm}_{L_w/K_v}(a_w)$.

Així, tenim que el diagrama

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{id} & I_L \\ \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{id} & I_K \end{array}$$

commuta i es pot transformar en un diagrama entre els grups de classes i els grups de classes idèlics.
A més, la inclusió dins el grup de classes idèlic també ens dóna un diagrama commutatiu de la forma següent:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathcal{C}_L & \longrightarrow & 0\ . \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathcal{C}_K & \longrightarrow & 0 \end{array}$$

Podem aplicar el lema de la serp per trobar una isomorfisme entre els idèles al fer quocient per els subgrups de norma: $\mathbb{I}_L/K^\times \,\mathrm{Nm}(\mathbb{I}_K) \cong \mathcal{C}_K/\,\mathrm{Nm}(\mathcal{C}_L)$.
La notació idèlica fa més fàcil pensar l'aplicació d'Artin en el cas global com un producte dels casos locals. Per exemple, si en l'extensió L/K tenim una plaça w en L per sobre d'una altra v a K, podrem aplicar els resultats del cas local per trobar una aplicació d'Artin de la forma

$$\phi_v : K_v^\times \to \mathrm{Gal}(L_w/K_v).$$

A més podem provar que aquesta aplicació no depèn de l'elecció del valora absolut en la plaça w. En particular, el subgrup $\mathrm{Gal}(L_w/K_v)$ equival al subgrup de descomposició que denotarem com D_w.

[14] Recordem que en un grup topològic, n'hi ha prou amb donar una base d'entorns d'un sol element ja que les traslacions són aplicacions contínues.

Proposició 5.2. Existeix un únic morfisme continu $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ amb la propietat de que per qualsevol $L \subset K^{\mathrm{ab}}$ i qualsevol plaça w sobre una altra v el següent diagrama

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & \mathrm{Gal}(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\phi_{v|L}} & \mathrm{Gal}(L/K) \end{array}$$

commuta.

Demostració. L'existència d'aquest morfisme la veiem, igual que en l'altra formulació, a través de l'existència dels morfismes en les subextensions finites, que veurem en les proves dels pròxims resultats. Així, l'aplicació es definirà a través de les aplicacions locals que hem vist en la secció anterior, en cada plaça. □

Teorema 5.5. (*Llei de reciprocitat en termes d'idèles*) El morfisme $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ té les següents propietats.

1. $\phi_K(K^\times) = 1$.
2. Per a qualsevol extensió abeliana finita L/K, ϕ_K defineix un isomorfisme
$$\phi_{L/K} : \mathbb{I}_K/(K^\times \mathrm{Nm}(\mathbb{I}_L)) \to \mathrm{Gal}(L/K).$$

Teorema 5.6. (*Teorema d'existència en termes d'idèles*) Fixada una clausura algebraica K^{al} del cos K, per a qualsevol subgrup obert d'index finit $N \subset \mathbb{C}_K$, existeix una única extensió abeliana L/K de manera que $N = \mathrm{Nm}_{L/K}(\mathbb{C}_L)$.

5.4 Equivalencia entre les dues formulacions

El propòsit d'aquesta secció és mostrar que les dues formulacions que hem presentat de la teoria global de cossos de classe són equivalents, algebraica i topològicament. Per això, és necessari veure que donada una aplicació $\psi : I^S \to G$ com les de la formulació clàssica, podem construir una en termes dels idèles de la forma $\phi : \mathbb{I}_{\mathfrak{m}} \to G$. No només això: també volem veure que les propietats topològiues que permeten, en la formulació idèlica, pensar en el cas global com a conseqüència del cas local, també es mantenen en la formulació clàssica. En altres paraules, que la aplicació ψ mencionada anteriorment és contínua, també ho és la corresponent ϕ, i viceversa. Per a fer tot això, necessitem unes quantes definicions preeliminars.

Definició 5.14. Donat un modulus $\mathfrak{m}$, per a cada $\mathfrak{p}$ que el divideixi podem definir com a entorn de l'1 els conjunts:

$$W_{\mathfrak{m}}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0} & \mathfrak{p} \text{ real} \\ 1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})} & \mathfrak{p} \text{ finit} \end{cases}.$$

Definició 5.15. Definim el grup d'idèles d'un modulus $\mathfrak{m}$ com:

$$\mathbb{I}_{\mathfrak{m}} = \Big(\prod_{\mathfrak{p}|\mathfrak{m}} K_v^\times \times \prod_{\mathfrak{p}\nmid\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \Big) \cap \mathbb{I}_K.$$

Definició 5.16. Definim el grup d'idèles d'unitats d'un modulus $\mathfrak{m}$ com:

$$W_{\mathfrak{m}} = \prod_{\mathfrak{p}\nmid\mathfrak{m} \ \mathfrak{p} \textbf{ infinit}} K_v^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \times \prod_{\mathfrak{p}\nmid\mathfrak{m} \ \mathfrak{p} \textbf{ finit}} U_{\mathfrak{p}}.$$

on $U_{\mathfrak{p}}$ són els entorns oberts de l'1 en el cos local.

Aquestes definicions ens permeten veure $K_{\mathfrak{m},1}$ en termes dels entorns de l'1 en el cos, i depenent del modulus. És a dir,

$$K_{\mathfrak{m},1} = K^\times \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p})$$

i per tant

$$K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_{\mathfrak{m}}.$$

També donen lloc a una caracterització del grup de classes radial d'un modulus $C_{\mathfrak{m}}$.

Proposició 5.3. La identitat $\mathrm{id} : \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ defineix un isomorfisme

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \cong C_{\mathfrak{m}}.$$

Demostració. Tenim una inclusió trivial de $K_{\mathfrak{m},1}$ dins $\mathbb{I}_{\mathfrak{m}}$ i una identificació entre $\mathbb{I}_{\mathfrak{m}}$ i $I^{S(\mathfrak{m})}$. Per tant, escrivim aquestes aplicacions de manera

$$K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$$

i apliquem el lema nucli-conucli. Sabem que el conucli de la primera aplicació és $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}$ i el de la composició és $C_{\mathfrak{m}}$. També sabem que la primera aplicació és injectiva. Només ens falta veure que el nucli de la segona aplicació és $W_{\mathfrak{m}}$ i ja tindrem factoritzada l'aplicació de la forma

$$W_{\mathfrak{m}} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to 0.$$

Prenem un element $a \in \mathfrak{I}_{\mathfrak{m}}$ que vagi a l'element neutre de $I^{S(\mathfrak{m})}$. Aleshores, en els primers que no estiguin a $\mathfrak{m}$, aquest element generarà l'ideal total, per tant estarà a $\mathcal{O}_{\mathfrak{p}}^{\times}$. En al resta de primers que sí que estiguin a $\mathfrak{m}$ tindrà valoració positiva $m(\mathfrak{p})$ (i això també funcionaria en el cas infinit) i per tant estarà a $1 + \mathfrak{p}^{m(\mathfrak{p})}$. Aquest argument també valdria per a veure l'altra inclusió. □

Proposició 5.4. La inclusió $i : \mathbb{I}_{\mathfrak{m}} \to \mathbb{I}_K$ defineix un isomorfisme

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m}} \cong \mathbb{I}_K/K^{\times}$$

Demostració. Partim de la inclusió $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}$ passa el quocient a $\mathbb{I}/K^{\times}$ de manera que el nucli és $K^{\times} \cap \mathbb{I}_{\mathfrak{m}} = K_{\mathfrak{m},1}$. Per tant, tenim una aplicació injectiva

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}/K^{\times}$$

Ens falta veure que també és exhaustiva. Prenem $\overline{a} = (a_v) \in \mathbb{I}$. Usant el teorema d'aproximació dèbil (2.2), i que el conjunt de primers que divideixen $\mathfrak{m}$ és finit, podem prendre $b \in K$ prou proper a a_v per totes les places que divideixin $\mathfrak{m}$. Podem escollir aquest b de manera que $\frac{a_v}{b}$ estigui prou proper de 1, o en altres paraules, que estigui en un entorn prou petit garantint $\frac{a_v}{b} \in W_{\mathfrak{m}}(\mathfrak{p})$. En les places reals també podem garantir el signe. Per tant, $\frac{\overline{a}}{b}$ té per imatge el nostre element idèlic inicial $\overline{a}$. □

Definició 5.17. Sigui S un conjunt finit de places que conté les places infinites de K, i sigui G un grup abelià finit. Diem que un morfisme

$$\psi : I^S \to G$$

admet un modulus si existeix un modulus $\mathfrak{m}$ tal que $\psi(i(K_{\mathfrak{m},1})) = 1$.

Proposició 5.5. Si $\psi : I^S \to G$ admet un modulus, aleshores existeix un únic morfisme tal que:

1. ϕ és contínua (prenent G amb la topologia discreta).
2. $\phi(K^{\times}) = 1$.
3. $\phi(a) = \psi(\mathrm{id}(a))$, en tots els $(a_v) \in \{a_v = 1 \text{ quan } v \in S\}$.

A part, tot morfisme continu que compleixi la segona propietat, prové d'algun ψ.

Demostració. En cas que el morfisme inicial admeti un modulus podem identificar S amb $S(\mathfrak{m})$. Així, el nostre és trivial a $K_{\mathfrak{m},1}$, el qual ens permet definir $\psi : C_{\mathfrak{m}} \to G$. Definim ara l'aplicació ϕ sobre $\mathbb{I}$, usant les proposicions anteriors i les projeccions sobre el quocient.

$$\phi : \mathbb{I} \to \mathbb{I}/K^{\times} \cong \mathbb{I}_m/K_{\mathfrak{m},1} \to \mathbb{I}_m/K_{\mathfrak{m},1}W_{\mathfrak{m}} \cong C_{\mathfrak{m}} \to G.$$

La última fletxa denota l'aplicació ψ. La propietat 2 es compleix per haver definit ϕ com un pas al quocient. La continuïtat és conseqüència de que qualsevol element de G, té per antiimatge un obert del tipus $W_{\mathfrak{m}}(\mathfrak{p})$. També veiem que en la propia definició, si prenem $\overline{a} \in \mathbb{I}_{\mathfrak{m}}$, com que en cap cas aquest element passara a ser trivial al quocient, tindrem $\phi(\overline{a}) = \psi(\overline{a})$. Per provar que aquesta aplicació ϕ vé únicament determinada

per les propietats 1,2,3, hem de veure que els idèles on coneixem el seu valor només mirant les propietats, $\mathbb{I}_S K^\times$, són densos en tot el grup $\mathbb{I}$: donat $\overline{a} = (a_v) \in \mathbb{I}$, el teorema d'aproximació dèbil ens permet prendre un $b \in K^\times$ que estigui prou proper a cada a_v amb $v \in S$. Així, ens podem construir un element $\overline{a'} \in \mathbb{I}_S$ que compleixi $a'_v b = a_v$ per tota $v \notin S$. Per tant, $\overline{a'}b \in \mathbb{I}_S$ i és prou proper a $\overline{a}$.
Ens falta comprovar que la propietat 2 és suficient per a que un morfisme continu ϕ provingui d'un com el ψ. Com que hem pres la topologia discreta en G, sabem que el nucli és un obert que conté l'1. Per tant, conté algun entorn $U(S, \varepsilon) \subset \operatorname{Ker}\phi$, per alguns S(finit),ε. Amb això, prenem un modulus $\mathfrak{m}$ que contingui totes les places de S i que en els seus primers finits compleix $1 + \mathfrak{p}^{m(\mathfrak{p})} = U_v$. També ens cal que en les seves places reals, la component connexa de K_v que contingui 1 sigui $\mathbb{R}_{>0}$. Aleshores, per a aquest modulus, $W_\mathfrak{m}$ està contingut en el nucli de ϕ. Per tant, partiem d'un morfisme $\phi : \mathbb{I} \to G$, que fent servir la segona propietat es restringeix a un altre morfisme $\overline{\phi} : \mathbb{I}/K^\times \to G$. Alhora, podem prendre com a domini $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}$ i com ja hem dit $W_\mathfrak{m}$ està en el nucli, i com a tal, passa a un morfisme en $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m} \cong C_\mathfrak{m}$. Només ens cal restringir-lo al morfisme exhaustiu de $I^S \to C_\mathfrak{m}$, que és com el ψ inicial i està unívocament determinat. □

Finalment ens caldria demostrar que, en els subgrups de norma idèlics, també hi podem encabir subgrups de la forma $W_\mathfrak{m}$. *Milne, CFT, 5.4.*

5.5 Cohomologia idèlica

Si $\sigma \in G$ i w és una valoració en L per sobre d'una fixada v, σw serà una nova valoració per sobre de v definida per $|a|_{\sigma w} = |\sigma^{-1}(a)|_w$. Amb aquests cossos tenim un diagrama commutatiu.

$$\begin{array}{ccc} L_w & \xrightarrow{\sigma} & L_{\sigma w} \\ {\scriptstyle i_w}\uparrow & & \uparrow{\scriptstyle i_{\sigma w}} \\ L & \xrightarrow{\sigma} & L \end{array}.$$

Per tant, podem pensar de manera simultània en totes les places que queden per sobre d'una fixada v. El que serà verdaderament interessant serà veure com actúa el grup de Galois sobre totes les places de L.

Proposició 5.6. Donades una valoració v en un cos K i K_v la compleció respecte aquesta valoració, prenem una extensió finita separable L/K i L_w totes les completacions tals que w està per sobre de v. Aleshores es té l'isomorfisme

$$L \otimes_K K_v \cong \prod_{w|v} L_w$$

donat per la fórmula $a \otimes b \to (i_w(a)b)_w$ on i_w és la inclusió del diagrama anterior.

Demostració. Per començar, prenem $\alpha \in L$ un element primitiu de l'extensió amb f el seu polinomi mínim. Aquest polinomi descompon a K_v de la manera $\prod_i f_i(X)$. Amb això podem construir la cadena d'isomorfismes

$$L \otimes_K K_v \cong K[\alpha] \otimes_K K_v \cong K_v[X]/(f(X)) \cong \prod_i K_v[X]/(f_i(X))$$

on l'isomorfisme del mig ve definit per $p(\alpha) \otimes \beta_v \to \overline{\beta_v p(\alpha)}$. □

El que hem de veure és en quins termes es dóna l'acció de Galois de G sobre $L^\times$.

Lema 5.4. Sigui $a = (a_w) \in \prod_{w|v} L_w$ i $\sigma \in G$. La fórmula

$$\sigma(a) = (\sigma(a_{\sigma^{-1}w}))$$

converteix $\prod_{w|v} L_w$ en un G-mòdul. Altrament, compleix les propietats.

1. Els elements de la forma $(a, \dots, a)$ amb $a \in K_v$ queden fixos per G.
2. Per cada $a \in L$, $\sigma(\dots, i_w(a), \dots) = (\dots, i_w(\sigma(a)), \dots)$.

Demostració. L'única part de la demostració que suposa dificultat és la segona propietat. Veiem que

$$\sigma(a) = (\sigma(a_{\sigma^{-1}w})) = \sigma(i_{\sigma^{-1}w}a) = (i_w(\sigma(a))$$

usant la commutativitat del diagrama anterior. □

Proposició 5.7. Sigui $w_0 \mid v$ i G_{w_0} el seu grup de descomposició. Per $a \in \prod_{w|v} L_w$ i $\sigma \in G$, definim $f_a(\sigma) = \sigma(a_{\sigma^{-1}w})$. Aleshores $f_a \in \mathrm{Ind}_{G_{w_0}}^G$ i l'aplicació $a \to f_a$ és un isomorfisme entre

$$\prod_{w|v} L_w \to \mathrm{Ind}_{G_{w_0}}^G .$$

El teorema també valdrà per altres G-mòduls $L_{w_0}^\times$ i U_w.

Demostració. Si $\rho \in G_{w_0}$, aleshores $\rho^{-1}w_0 = w_0$.

$$f_a(\rho\sigma) = \rho\sigma(a_{\sigma^{-1}\rho^{-1}w_0}) = \rho f_a(\sigma)$$

Per tant $f_a \in \mathrm{Ind}_{G_{w_0}}^G$. A més, f_a també actuarà com a morfisme de G-mòduls.

$$\tau f_a(\sigma) = f_a(\sigma\tau) = \sigma\tau(a_{\tau^{-1}\sigma^{-1}w_0}) = \sigma(\tau a_{\sigma^{-1}w_0}) = f_{\tau a}(\sigma)$$

Per veure la bijectivitat podem construir la seva inversa. Donada una $f \in \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})$, construim $a^f \in \prod_{w|v} L_w$ de manera que en la plaça w val $a_w^f = \sigma(f(\sigma^{-1}))$ prenent σ tal que $w = \sigma w_0$. Vegem que efectivament actua com l'aplicació inversa en els dos sentits:

$$f_{a^f}(\tau) = \tau(a^f_{\tau^{-1}w_0}) = f(\tau);$$

$$a_w^{f_a} = \sigma(f_a(\sigma^{-1})) = a_w.$$

□

Proposició 5.8. Per a tot $r \geq 0$,

$$H^r(G, \prod_{w|v} L_w) = H^r(G_{w_0}, L_{w_0}).$$

Demostració. Per demostrar això només hem d'aplicar el lema de Shapiro:

$$H^r(G, \prod_{w|v} L_w) = H^r(G, \mathrm{Ind}_{G_{w_0}}^G(L_{w_0})) = H^r(G_{w_0}, L_{w_0}).$$

Cal notar que l'isomorfisme près és independent de l'elecció de la plaça w_0. En particular,

$$H^0(G, \prod_{w|v} L_w) = K_v^\times.$$

També cal dir que tenim resultats anàlegs per a les unitats U_v. □

Aquests resultats ja ens permeten coneixer l'acció del grup de Galois sobre els idèles, i per tant construir la cohomologia dels idèles com a suma directa de cadascuna de les places.

Proposició 5.9. Per a tot $r \geq 0$,

$$H^r(G, \mathbb{I}_L) = \bigoplus_v H^r(G_v, L_v^\times)$$

on $L_v^\times = L_w^\times$ per una plaça qualsevol, i G_v és el grup de descomposició en aquesta plaça.

Demostració. Prenem un conjunt de places qualsevol S i $\mathbb{I}_{S,L} = \prod_{v\in S}\prod_{w|v} L_w^\times \times \prod_{v\notin S}\prod_{w|v} U_w$. Es pot demostrar que $\varinjlim_S H^r(G,\mathbb{I}_{S,L}) = H^r(G,\mathbb{I}_L)$. A partir d'aquí, veiem que

$$H^r(G,\mathbb{I}_{S,L}) = \prod_{v\in S}\prod_{w|v} H^r(G_v, L_v^\times) \times \prod_{v\notin S}\prod_{w|v} H^r(G_v,U_v) = \prod_{v\in S}\prod_{w|v} H^r(G_v,L_v^\times)$$

sabent que la cohomologia de les unitats és nula com ja hem vist al lema 4.1.

$$H^r(G,\mathbb{I}_L) = \varinjlim_S \bigoplus_{v\in S} H^r(G_v,L_v^\times) = \bigoplus_v H^r(G_v,L_v^\times).$$

□

Això ens permet veure que $H^1(G,\mathbb{I}_L) = 0$ (usant el teorema 90 de Hilbert) i que $H^2(G,\mathbb{I}_L) = \bigoplus_v \mathbb{Z}/n_v\mathbb{Z}$, on n_v és el grau de l'extensió local L_v/K_v. Com que en la majoria de les places l'extensió local serà trivial, podrem calcular H^2 de manera bastant explícita. De manera colateral també obtenim el quocient de Herbrand $h(\mathbb{I}_S) = \prod_v n_v$.
Amb això ja tenim estudiada la cohomologia per als idèles, que podrem calcular en funció de les cohomologies en cadascuna de les places. També ens faltaria analitzar la cohomologia per a les unitats als idèles.

Definició 5.18. Sigui L/K una extensió finita amb grup de Galois G i S un conjunt finit de places de K que conté les places infinites amb T les places que queden per sobre de S a L. Definim el grup de les T-unitats

$$U(T) = \{\alpha \in L\,,|\ \mathrm{ord}_w(\alpha) = 0\,\forall w \notin T\}.$$

Proposició 5.10. Sigui G grup de Galois d'una extensió L/K, amb les condicions dels resultats anteriors. Aleshores $h(U(T))$ està definit i ve donat per la formula

$$nh(U(T)) = \prod_{v\in S} n_v$$

on $n = [L:K]$ i $n_v = [L_v : K_v]$.

Demostració. Deixarem sense provar aquest últim resultat, ja que requereix més contingut previ d'àlgebra commutativa. *Milne, CFT, 7* □

5.6 Teoria de Kummer

Aquest incís sobre teoria de Kummer el farem servir en la següent secció on veurem els resultats necessàris per a poder definir la aplicació d'Artin sobre el nostre cos.

Definició 5.19. Diem que un grup de exponent n si $g^n = 1$ per tots els seus elements. Diem que una extensió de Galois L/K té exponent n si el seu grup de Galois té exponent n.

Ens referim a la teoria de Kummer d'un cos K com la construcció d'una bijecció entre les extensions d'exponent n i els subgrups de $K^\times/K^{\times n}$.
Sigui L/K una extensió finita de Galois. Tenim una successió exacta de la forma

$$1 \to \mu_n^L \to L^\times \xrightarrow{x\to x^n} L^{\times n} \to 1$$

on μ_n^L són tots els elements que són arrels n-èssimes de la unitat a L.
Notarem com $K^\times \cap L^{\times n}/K^{\times n}$ el grup dels elements de $K^\times$ que esdevenen potències n-èssimes a L. Podem usar la cohomologia per passar a una nova successió de la forma

$$0 \to \mu_n^K \to K^\times \xrightarrow{x\to x^n} K^\times \cap L^{\times n} \to H^1(G,\mu_n^L) \to 0.$$

El 0 al final prové del teorema 90 de Hilbert. L'acció de G sobre les arrels de la unitat és trivial. Aleshores, la successió anterior es pot transformar en un isomorfisme canònic

$$K^\times \cap L^{\times n}/K^{\times n} \cong \mathrm{Hom}(G,\mu_n^L).$$

En particular, l'isomorfisme envia un element $a \in K^\times \cap L^{\times n}/K^{\times n}$ al morfisme que envia $\sigma \to \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}$. Amb això també es pot veure que $\mathrm{Hom}(G,\mu_n^L)$ té ordre n, fet que necessitarem per al següent teorema que classifica les nostres extensions.

Teorema 5.7. L'aplicació que envia l'extensió L al grup $K^\times \cap L^{\times n}/K^{\times n}$ és una bijecció entre les extensions d'exponent n de K i els subgrups finits de $K^\times/K^{\times n}$. L'aplicació inversa la construim enviant un subgrup $B \subset K^\times/K^{\times n}$ a l'extensió $K[B^{\frac{1}{n}}]$ que conté una arrel n-èssima de cada element de B.

Demostració. Sigui L/K una extensió finita d'exponent n. Definim $B(L) = K^\times \cap L^{\times n}$. Podem veure la inclusió $L \supset K[B(L)^{\frac{1}{n}}]$.

$$x \in B(L)^{\frac{1}{n}} \Rightarrow \exists a \in B(L) \text{ tal que } a = x^n \Rightarrow a \in L^{\times n} \Rightarrow x \in L.$$

També tenim que per qualsevol subgrup $B \subset K^\times/K^{\times n}$ es té la inclusió $B(K[B^{\frac{1}{n}}]) \supset B$.

$$x \in B \to a \in B^{\frac{1}{n}} \text{ tal que } a^n = x \Rightarrow x \text{ té una arrel } n\text{-èssima a } K[B^{\frac{1}{n}}] \Rightarrow x \in B(K[B^{\frac{1}{n}}]).$$

Ara podem argumentar amb els índex i els graus de manera que

$$[L : K] \geq [K[B(L)^{\frac{1}{n}}] : K] = [B(K[B(L)^{\frac{1}{n}}]) : K^{\times n}] \geq [B(E) : F^{\times n}].$$

Si l'extensió és d'exponent n, aleshores es té la igualtat amb els índex per tant $L = K[B(L)^{\frac{1}{n}}]$. Idènticament, prenem $B \subset K^\times/K^{\times n}$ i prenem l'extensió $L = K[B^\times]$ a la qual li podem aplicar l'isomorfisme anterior. Usant la inclusió que ja teníem es veu que la imatge de B és un subgrup $\mathrm{Hom}(G/H, \mu_n^L) \subset \mathrm{Hom}(G, \mu_n^L)$. Però tal i com hem definit l'isomorfisme, H contindrà tots els elements σ tals que $\frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}} = 1$ amb $a \in B$. Per tant, σ fixarà els elements $a^{\frac{1}{n}}$, però aquests només poden ser trivials. Per tant,

$$H = 1 \Rightarrow \mathrm{Hom}(G/H, \mu_n^L) = \mathrm{Hom}(G, \mu_n^L) \Rightarrow B = B(E) = B(F[B^{\frac{1}{n}}]).$$

Amb aquestes dues igualtats, tenim que la nostra aplicació és una bijecció que a més conserva l'índex i el grau. □

5.7 La primera desigualtat

El propòsit de la següent secció és mostrar la igualtat entre els ordres dels dos grups de l'aplicació d'Artin per veure que es pot definir com el producte de les aplicacions locals en cada plaça. Per tant, hem de demostrar la igualtat

$$[\mathbb{I}_K : K^\times \mathrm{Nm}(\mathbb{I}_L)] = [\mathcal{C}_K : \mathrm{Nm}(\mathcal{C}_L)] = [L : K].$$

La primera desigualtat és $[\mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L)] \geq [L : K]$. Començarem a demostrar-la partint de l'esquema que ja hem vist anteriorment.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L^\times & \longrightarrow & \mathbb{I}_L & \longrightarrow & \mathcal{C}_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \downarrow{\scriptstyle \mathrm{Nm}_{L/K}} & & \\ 0 & \longrightarrow & K^\times & \longrightarrow & \mathbb{I}_K & \longrightarrow & \mathcal{C}_K & \longrightarrow & 0 \end{array}$$

Aquest esquema dóna una identificació entre $\mathcal{C}_K$ i $H^0(G, \mathcal{C}_L) = \mathcal{C}_L^G$. Sabent això podem escriure el quocient de Herbrand per a $\mathcal{C}_L$ com

$$h(\mathcal{C}_L) = \frac{[\mathcal{C}_K : \mathrm{Nm}(\mathcal{C}_L)]}{H^1(G, \mathcal{C}_L)}.$$

Recordem que $\mathcal{C}_K$ és un grup finit. Basant-nos en aquest resultat podrem prendre conjunts de places finits que continguin tots els generadors del grup de classes.

Lema 5.5. Sigui K un cos de nombres i sigui S un conjunt finit de places que contingui un conjunt de generadors del grup de classes. Aleshores, en termes d'idèles, tenim que

$$\mathbb{I}_K = K^\times \mathbb{I}_S.$$

Demostració. Per com hem construit S, qualsevol ideal fraccionari $\mathfrak{a}$ es pot escriure com $\mathfrak{b}(c)$ amb $\mathfrak{b} \in \langle S \rangle$ i $c \in K^\times$. Per tant, $\mathfrak{a}$ esdevé un ideal principal al quocient $I_K/\langle S \rangle$ o el que és el mateix $I_K^S/i(K^\times) = 0$. Passant del grup de classes als idèles trobem $\mathbb{I}_K/K^\times \mathbb{I}_S \cong I_K^S/i(K^\times) = 0$. □

Teorema 5.8. Per qualsevol extensió cíclica finita L/K, $h(\mathcal{C}_L) = [L : K]$.

Demostració. Prenem un conjunt finit de places S de K que contingui les places infinites, contingui també totes aquelles places que siguin ramificades en la part local (que només poden ser un nombre finit) i finalment un conjunt de generadors del grup de classes. Sigui T el conjunt de places de L per sobre de S. Llavors

$$\mathcal{C}_L = \mathbb{I}_L/L^\times = L^\times \mathbb{I}_T/L^\times \cong \mathbb{I}_T/L^\times \cap \mathbb{I}_T.$$

En aquests últims isomorfismes hem aplicat el lema anterior i el segon teorema d'isomorfisme. També tenim que

$$L^\times \cap \mathbb{I}_T = U(T)$$

ja que aquest grup consisteix a tots els elements idèlics que tenen ordre 0 fora de les places de T. Ara, aplicant les proporcions del quocient de Herbrand veiem que

$$0 \to U(T) \to \mathbb{I}_T \to \mathbb{I}_T/U(T) \to 0,$$

i obtenim, aplicant la proposició 5.10, que

$$h(\mathcal{C}_L) = \frac{h(\mathbb{I}_T)}{h(U(T))} = \frac{nh(\mathbb{I}_T)}{\prod_{w\in T} n_v} = n.$$

□

Corol·lari 5.3. Per qualsevol extensió cíclica finita de grau n

$$[\mathbb{I}_K : K^\times \operatorname{Nm}(\mathbb{I}_L)] \geq n.$$

Demostració. El numerador del quocient de Herbrand ha de ser més gran que n. Per tant, $[\mathcal{C}_K : \operatorname{Nm}(\mathcal{C}_L)] \geq n$. □

Anem a trobar ara algunes aplicacions d'aquesta desigualtat que ens permetran veure les primeres propietats del que en el futur serà la nostra aplicació d'Artin.

Proposició 5.11. Sigui L/K una extensió finita i resoluble. Si existeix un subgrup $D \subset \mathbb{I}_K$ tal que:

1. $D \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L)$;
2. $K^\times D$ és dens a $\mathbb{I}_K$.

Aleshores, $L = K$.

Demostració. Com que l'extensió és resoluble, tenim algun subcos $K \subset K' \subset L$ que sigui cíclic sobre K. Usant les propietats de D,

$$D \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L) = \operatorname{Nm}_{K'/K}(\operatorname{Nm}_{L/K'}(\mathbb{I}_L)) \subset \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'})$$

amb el qual tenim que $K^\times \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'})$ també és dens a $\mathbb{I}_K$. Com que també és un subgrup, és tancat en la topologia dels idèles, i a més és unió arbitrària d'oberts $K^\times \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'}) = \cup_{x\in K} x \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'})$. Per tant, un obert, tancat i dens ha de ser el total, amb el qual $\mathbb{I}_K = K^\times \operatorname{Nm}_{K'/K}(\mathbb{I}_{K'})$. Usant la primera desigualtat, tenim que aquesta extensió és trivial, $K' = K$. Repetint aquest proces per totes les extensions cícliques en la torre cíclica de L, arribarem a $L = K$. □

Proposició 5.12. Donada una extensió resoluble no trivial L/K, existeixen infinites places que no descomponen completament.

Demostració. Suposem que hi ha un nombre finit de places que no descomponen completament dins un conjunt S. Demostrarem que es donen les propietats de la proposicó anterior per a

$$D = \mathbb{I}_S = \{(a_v) \,|\, a_v = 1 \text{ per a } v \in S\}.$$

Les extensions que descomponguin completament, a nivell de cossos locals, seràn trivials ja que $e = f = 1$. Per tant, $D \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L)$ ja que fora de S, l'extensió és trvial i a S els elements de D són trivials. Pel que fa la densitat, fem servir l'anomenat teorema d'aproximació dèbil, que ens dóna aproximació d'elements per valoracions. Amb això apliquem la proposició anterior i arribem a contradicció amb $L \neq K$. □

Proposició 5.13. Per qualsevol extensió resoluble finita L/K i conjunt de places T que contingui aquelles que ramifiquin, el conjunt dels elements de Frobenius $(\mathfrak{P}, L/K)$ per $\mathfrak{P} \notin T$ genera el grup $G = \mathrm{Gal}(L/K)$.

Demostració. Sigui $H \subset G$ el grup que generin aquests elements i $E = L^H$ el cos fix per H. Per tant, els elements $(\mathfrak{P}, E/K) = (\mathfrak{P}, L/K)_{|E}$ són trivials. Per tant, totes les places fora de T són trivials, amb el qual $E = K$ per els resultats anteriors. Amb això, per la correspondència de Galois, tenim $H = G$. □

Amb això ja podem construir un conjunt finit de places fora d'aquelles que descomponen que generin el grup de Galois.

5.8 La segona desigualtat

La segona desigualtat l'enunciarem dins un teorema més general, que ilustra que demostrar-la és el mateix que demostrar que $H^2(G, L)$ és un grup cíclic d'ordre n. Per tant, per demostrar la llei de reciprocitat, podríem també usar el teorema de Tate com en el cas local. A partir d'aquí, ens restringirem a casos particulars que redueixin la problemàtica de la desigualtat.

Teorema 5.9. Sigui L/K una extensió finita de grau n amb grup de Galois G. Aleshores, qualseol de les tres condicions següents es compleix.

1. La segona desigualtat: $[\mathbb{I}_K : K^\times \mathrm{Nm}(\mathbb{I}_L)]$ divideix n.
2. $H^1(G, \mathcal{C}_L) = 0$;
3. $H^2(G, \mathcal{C}_L)$ és cíclic d'ordre dividint n.

Lema 5.6. Si G és cíclic, les tres condicions del teorema anterior són equivalents.

Demostració. Si el grup és cíclic podem aplicar la periodicitat dels grups de Tate per obtenir $\mathbb{I}_K/K^\times \mathrm{Nm}(\mathbb{I}_L) = H^0_T(G, \mathcal{C}_L) \cong H^2_T(G, \mathcal{C}_L)$ el qual fa equivalents les propietats 1 i 3. Sabent que $h(\mathcal{C}_L) = n$, si el numerador divideix n, el denominador ha de ser trivial, i viceversa, amb $H^1(G, \mathcal{C}_L) = 0$, el qual fa equivalents les condicions 1, 3 amb la condició 2. □

Lema 5.7. És suficient provar el teorema per a G un p-grup de Galois d'una extensió L/K.

Demostració. Apliquem el corol·lari 3.4 i restringim de manera injectiva sobre la cohomologia d'un subgrup de Sylow G_p. Obtenim que la aplicació restricció

$$\mathrm{Res} : H^r_T(G, \mathcal{C}_L) \to H^r(G_p, \mathcal{C}_L)$$

és injectiva sobre les components p-primàries de $H^r_T(G, \mathcal{C}_L)$. Pel teorema d'Artin[15], l'extensió L/L^{G_p} té grup de Galois G_p que té ordre potència de p. Aleshores, per tot p que divideixi $[L : K]$, $|H^2(G, \mathcal{C}_L)|$ divideix $|H^2(G_p, \mathcal{C}_L)|$ que per hipòtesi divideix la potència màxima de p en $[L : K]$. També es poden veure les altres dues condicions. Cal repetir el raonament per a tots els p que divideixin el grau i obtindrem el que volem. □

Lema 5.8. És suficient provar el teorema amb G un grup de Galois cíclic d'ordre primer d'una extensió L/K.

Demostració. Podem suposar G un p-grup pel lema anterior. Demostrarem el resultat per inducció sobre n quan p^n és l'ordre de G. El cas base és la nostra suposició. En potències superiors, podem aplicar el teorema de Sylow i agafar H un subgrup de G d'ordre p. Ara apliquem la successió del teorema 3.1.

$$0 \to H^r_T(G/H, \mathcal{C}_L) \xrightarrow{\mathrm{Inf}} H^r_T(G, \mathcal{C}_L) \xrightarrow{\mathrm{Res}} H^r_T(H, \mathcal{C}_L).$$

Per inducció, $H^1_T(G/H, \mathcal{C}_L) = 0$ i pel lema anterior $H^1_T(H, \mathcal{C}_L) = 0$. □

Lema 5.9. És suficient provar la segona desigualtat en el cas que el cos base K contingui una arrel p-èssima de la unitat.

[15] Aquest resultat afirma que si G és un subgrup dels automorfismes d'un cos L i prenem el cos fix per aquest subgrup L^H, aleshores l'extensió L/L^H és de Galois amb grup de Galois G

Demostració. Sigui $K' = K[\zeta]$ que té ordre $m|p-1$. Com que l'extensió L/K és de grau p, prenem $L' = K'L$ i tindrem el següent esquema

$$\begin{array}{ccc} L & \xrightarrow{m} & L' \\ {\scriptstyle p}\uparrow & & \uparrow{\scriptstyle p} \\ K & \xrightarrow{m} & K' \end{array}$$

on les extensions L i K' són disjuntes, i per tant podrem generar el grup de Galois de L' com a producte de les dues subextensions,

$$\mathrm{Gal}(L'/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K).$$

De l'esquema de cossos podem passar a un esquema de grups de classes idèlics de la forma següent.

$$\begin{array}{ccccccc} \mathcal{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \mathcal{C}_K & \longrightarrow & \mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L) & \longrightarrow & 0 \\ \downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\ \mathcal{C}_{L'} & \xrightarrow{\mathrm{Nm}_{L'/K'}} & \mathcal{C}_{K'} & \longrightarrow & \mathcal{C}_{K'}/\mathrm{Nm}(\mathcal{C}_{L'}) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \mathrm{Nm}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{Nm}_{K'/K}} & & \downarrow & & \\ \mathcal{C}_L & \xrightarrow{\mathrm{Nm}_{L/K}} & \mathcal{C}_K & \longrightarrow & \mathcal{C}_K/\mathrm{Nm}(\mathcal{C}_L) & \longrightarrow & 0 \end{array}$$

Com que les extensions són disjuntes tenim isomorfismes també a $\mathrm{Gal}(L'/L) \cong \mathrm{Gal}(K'/K)$ i $\mathrm{Gal}(L'/K') \cong \mathrm{Gal}(L/K)$, i això ens dóna la commutativitat del diagrama, ja que les normes commuten amb les inclusions. En particular, les dues primeres columnes del diagrama actuaran com la multiplicació per m ja que estem prenent la norma d'elements del cos base. Usant la commutativitat, també la tercera columna equivaldrà a la multiplicació per m. Però al estar multiplicant per m, que és coprimer amb p, l'aplicació és un isomorfisme. En particular,

$$[\mathcal{C}_K : \mathrm{Nm}(\mathcal{C}_L)] \text{ divideix } [\mathcal{C}_{K'} : \mathrm{Nm}(\mathcal{C}_{L'})]$$

i aquest últim nombre estem assumint que divideix p. □

Sabem que K conté una arrel p-èssima primitiva de la unitat. Per tant, a partir d'ara podem suposar que L/K és una extensió abeliana de grau p^r, per tant d'exponent p amb grup de Galois $G = \left(\mathbb{Z}/p\mathbb{Z}\right)^r$ que per teoria de Kummer sabem que és de la forma $L = K[a_1^{\frac{1}{p}}, \ldots, a_r^{\frac{1}{p}}]$. Prenem ara S un conjunt finit de places de K que compleixi la següent llista de propietats.

1. S conté les places infinites.
2. S conté les places per sobre de p. [16]
3. Els a_i són tots S-unitats, per tant només admeten denominadors a S.
4. S conté un conjunt de generadors del grup de classes, i per tant compleix $\mathbb{I}_K = \mathbb{I}_S K^\times$.

Usant el teorema de les unitats de Dirichlet, *Milne, ANT, 5* podem demostrar que el grup $U(S)$ té rang $s-1$ on $s = |S|$. A més, el grup de torsió $U(S)_{\text{torsio}}$ és cíclic i p divideix el seu ordre, ja que conté les arrels p-èssimes de la unitat. Amb això, podem veure que

$$U(S)/U(S)^p \cong \left(\mathbb{Z}/p\mathbb{Z}\right)^r$$

Amb això podem construir una nova extensió finita M/K de manera que $M = K[U(S)^{\frac{1}{p}}]$, és a dir, estem afegint totes les arrels p-èssimes dels elements de $U(S)$, que és finitament generat. Tornant a usar teoria de Kummer podem veure que correspon al grup $\left(\mathbb{Z}/p\mathbb{Z}\right)^s$. En particular, $K \subset^{p^r} L \subset^{p^t} M$ amb $r+t = s$.

Proposició 5.14. Existeix un altre conjunt finit de places T de K, de manera que

$$\{(\mathfrak{P}, M/K) \,|\, v \in T\}$$

és un conjunt de generadors del grup $\mathrm{Gal}(M/L) = \left(\mathbb{Z}/p\mathbb{Z}\right)^t$.

[16] Recordem que tota l'estona estem treballant amb un cos de nombres, és a dir, una extensió finita de $\mathbb{Q}$.

Demostració. Les places que no ramifiquin estaran fora de S. Usant, que el coeficient $e = 1$ i l'extensió és de grau potencia de p, veiem que la part local en les places $v \notin S$ serà M_w/K_v, cíclica de grau p o trivial, amb $w|v$. Per tant, no hi pot haver cap extensió intermèdia L_w no trivial.
Usant la proposició 5.13, prenem T' un conjunt de places de L que generin $\mathrm{Gal}(M/L)$, i que cap d'elles divideixi a una plaça de L. Prenem una d'aquestes places $w \in T'$ i mirem com són les extensions locals sobre les places w_L de L i w_K de K. Però hem dit que no podia haver-hi cap extensió intermèdia, per tant $L_{w_L} = K_{w_K}$. Com a tal, el conjunt d'elements de Frobenius que estem prenent generarà el grup de Galois de l'extensió M/K. □

Proposició 5.15. Sota les condicions del lema anterior, prenem $a \in U(S)$. Aleshores, a és una potència p-èssima a L, si i només si, és una potència p-èssima a K_v per tot $v \in T$.

Demostració. En una direcció, si $a \in U(S)$ és una potència p-essima a L, aleshores ho és a L_w per tota plaça de L. En particular, per les places $w|v \in T$, l'extensió local és trivial i $L_w = K_v$. Per tant, també és una potència p-èssima a K_v.
En l'altre direcció, tenim $a^{\frac{1}{p}} \in M$. Si aquest element pertany a K_v per tota $v \in T$ aleshores el fixen els Frobenius $(\mathfrak{p}_v, M/K)$, però aquests generen tot el grup $\mathrm{Gal}(M/L)$, per tant aquest grup també el fixa i $a^{\frac{1}{p}} \in L$. □

Lema 5.10. El subgrup

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^{\times} \times \prod_{v \notin S \cup T} U_v$$

de $\mathbb{I}_K$ està contingut en les normes $\mathrm{Nm}_{L/K}(\mathbb{I}_L)$.

Demostració. Prenem $\mathfrak{d} \in E$. Hem de demostrar que és una norma en cadascuna de les places. Primerament, tenim l'isomorfisme de la teoria local

$$K_v^{\times} / \mathrm{Nm}_{L_w/K}(L_w^{\times}) \cong \mathrm{Gal}(L_w/K_v).$$

Com que el segon grup té exponent p, també ho faran en el primer, per tant $K_v^{\times p} \subset \mathrm{Nm}_{L_w/K}(L_w^{\times})$.
Per $v \in T$, les extensions locals són trivials, per tant tots els elements són normes.
Per a $v \notin S \cup T$, tenim les places no ramificades. Aqui tindrem que l'aplicació norma sobre les unitats és exhaustiva. □

Com a conseqüència d'aquest lema, ens hem de reduir a demostrar que $[\mathbb{I}_K : K^{\times} E]$ divideix l'ordre p^r, ja que el nostre índex $[\mathbb{I}_K : K^{\times} \mathrm{Nm}_{L/K}(\mathbb{I}_L)]$ dividirà aquest nombre. En particular, el lema 5.4 ens reduirà aquest índex a

$$[\mathbb{I}_K : K^{\times} E] = [K^{\times} \mathbb{I}_{S \cup T} : K^{\times} E].$$

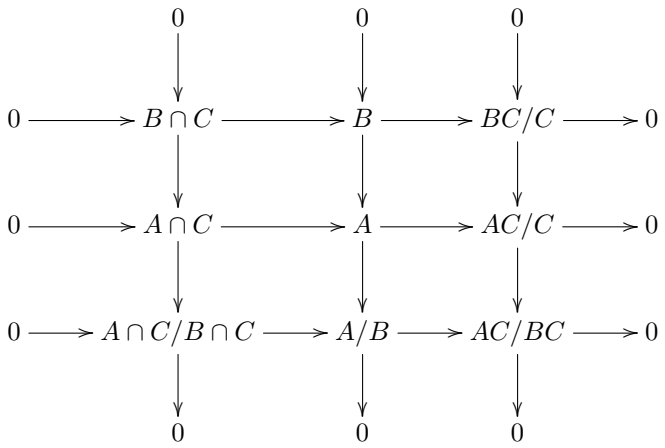
Reduirem aquest càlcul a dos índexs que sapiguem calcular.

Lema 5.11. Siguin A, B, C tres subgrups d'un grup abelià complint que $A \supset B$. Aleshores

$$[AC : BC][A \cap C : B \cap C] = [A : B],$$

de manera que si dos dels índex són finits, el tercer també ho és i compleix la igualtat.

Demostració. Usant el segon teorema d'isomorfisme, podem construir el següent diagrama



Sabem a priori que les dues primeres files són exactes. Per tant, aplicant els resultats d'àlgebra homològica, la successió de la tercera fila també és exacta i per tant el producte dels ordres laterals dóna l'ordre del mig. □

Apliquem aquest lema als idèles, amb $A = \mathbb{I}_{S\cup T}$, $B = E$, $C = K^\times$. Llavors

$$[\mathbb{I}_K : K^\times E] = \frac{[\mathbb{I}_{S\cup T} : E]}{[U(S\cup T) : K^\times \cap E]}.$$

Estudiarem per separat els valors del numerador i del denominador.

Lema 5.12. Es compleix la igualtat

$$[\mathbb{I}_{S\cup T} : E] = p^{2s}.$$

Per calcular aquest índex usarem aquest lema.

Proposició 5.16. Sigui K_v un cos local de característica 0 que contingui el grup μ_n de les arrels n-èssimes de la unitat. Aleshores,

$$[K^\times : K^{\times n}] = n\frac{|\mu_n|}{|n|_v}.$$

Si v és una valoració no arquimediana i U_v el seu subgrup d'unitats, aleshores

$$[U_v : U_v^n] = \frac{|\mu_n|}{|n|_v}.$$

Demostració. Les valoracions arquimedianes són les complexes i les reals. Si $K = \mathbb{C}$, μ_n té n elements i v és la norma complexa al quadrat; per tant, en tots dos costats, l'equació es redueix a $1 = n\frac{n}{n^2}$. Si $K = \mathbb{R}$, i n és imparell μ_n és trivial i la norma és la norma real, per tant l'equació val $1 = n\frac{1}{n}$; en el cas parell μ_n té 2 elements i l'equació val $2 = n\frac{2}{n}$. Passem al cas arquimedià, on ja hem vist que tenim $K_v \cong U_v \times \mathbb{Z}$. Per tant, tenim

$$[K_v : K_v^n] = [U_v : U_v^n] \cdot [\mathbb{Z} : n\mathbb{Z}],$$

i només hem de provar la segona part de la proposició. Per fer-ho, definim un anàleg al quocient de Herbrand

$$h_n(U_v) = \frac{[U_v : U_v^n]}{|U_n|},$$

on U_n és el subgrup de n-torsió, que en aquest cas equival a les arrels de la unitat. Usant l'isomorfisme exponencial que hem vist en el lema 4.2 de la secció anterior, podem pensar aquest quocient al grup additiu $\mathcal{O}_K$ i obtenim el que volem.

$$[U_v : U_v^n] = h_n(U)|U_n| = h_n(\mathcal{O}_K)|\mu_n| = [\mathcal{O}_K : n\mathcal{O}_K]|\mu_n| = \frac{|\mu_n|}{|n|_v}$$

□

Demostració. (*del lema 5.12*) Les úniques places en que l'índex és no trivial són les de S, de manera que

$$[\mathbb{I}_{S\cup T} : E] = \prod_{v\in S} [K_v^\times : K_v^{\times p}].$$

Per la proposició anterior, i usant que el cos conté les arrels p-èssimes de la unitat.

$$[\mathbb{I}_{S\cup T} : E] = \prod_{v\in S} \frac{p^2}{|p|_v} = \frac{p^{2s}}{\prod_{v\in S}|p|_v} = \frac{p^{2s}}{\prod_{\text{all } v}|p|_v} = p^{2s}.$$

□

Lema 5.13. Es compleix la igualtat

$$[U(S\cup T) : K^\times \cap E] = p^{s+t}.$$

Demostració. És evident que $K^\times \cap E \supset U(S\cup T)^p$. També que l'índex en les potències és el que volem pel teorema de les unitats de Dirichlet: $[U(S\cup T) : U(S\cup T)^p] = p^{s+t}$. Per tant, reduim la prova del nostre teorema a veure que $K^\times \cap E \subset U(S\cup T)^p$. Això ho demostrarem amb els dos següents lemes. □

Lema 5.14. Amb la notació usada anteriorment, l'aplicació canònica

$$U(S) \to \prod_{v\in T} U_v/U_v^p$$

és exhaustiva.

Demostració. Pel teorema d'isomorfisme, provar l'exhaustivitat equival a veure la igualtat entre l'ordre del conjunt d'arribada i l'índex del nucli. Sigui H aquest nucli, volem provar

$$[U(S) : H] = \prod_{v\in T} [U_v : U_v^p]$$

Per la proposició 5.12 i el fet que T i S són disjunts i per tant $|p|_v$ per $v \in t$, obtenim que la part esquerra val p^t. Altrament, per la proposició 5.11, el nucli és $H = U(S)\cap L^{\times p}$. Ara podem aplicar teoria de Kummer per veure

$$U(S)/H = U(S)/U(S)\cap L^{\times p} = U(S)L^{\times p}/L^{\times p},$$

on aquest últim subgrup correspon a una extensió de Kummer del grau que volem. □

Lema 5.15. Sigui K un cos que contingui una arrel n-èssima de la unitat i siguin S, T dos conjunts que compleixin les propietats que hem exigit anteriorment (S té prous places i T permet que es compleixi el lema anterior). Sigui $b \in K$ una potència n-èssima a K_v per tot $v \in S$ i una unitat fora de $S\cup T$. Aleshores, $b \in K^{\times n}$.

Demostració. Usarem la proposició 5.12 per veure que $L = K[b^{\frac{1}{n}}] = K$. El subgrup D que farem servir és

$$D = \prod_{v\in S} K_v^\times \times \prod_{v\in T} U_v^n \times \prod_{v\notin S\cup T} U_v.$$

Aquest resultat ens diu que n'hi ha prou amb veure dues condicions: $D \subset \mathrm{Nm}_{L/K}(\mathbb{I}_L)$ i $DK^\times = \mathbb{I}_L$. Prenem un element idèlic $= (d_v) \in D$ i veurem que és una norma en cada plaça.

1. $v \in S$. $K_v = K_v[b^{\frac{1}{n}}]$ per hipòtesi, per tant, tot element és una norma.
2. $v \in T$. Per la llei de reciprocitat local, l'índex $[K_v^\times : \mathrm{Nm}(K_v[b^{\frac{1}{n}}])]$ és igual al grau $[K_v[b^{\frac{1}{n}}] : K_v]$, que és n. Per tant, tota potència n-èssima és una norma.
3. $v \notin S\cup T$. nb és una unitat, per tant l'extensió $K_v[b^{\frac{1}{n}}]$ és no ramificada. Tal i com vem construir els subgrups de norma en les extensions locals, tota unitat aquí és una norma.

Per a la segona condició, prenem l'idèle $\mathbb{I}_S$ i per la seva definició és evident que $\mathbb{I}_S/D = \prod_{v\in T} U_v/U_v^n$. Usant la hipòtesi de exhaustivitat veiem que $\mathbb{I}_S = DU(S)$. Usem també la condició de que conté generadors del grup de classes, i llavors fem serivr el lema 5.4 i veiem

$$\mathbb{I}_K = \mathbb{I}_S K^\times = DU(S)K^\times = DK^\times,$$

que finalitza la prova del resultat. □

Aquest últim resultat reformula la inclusió que voliem veure $K^\times \cap E \subset U(S\cup T)^p$. Doncs, els càlculs que acabem de fer acaben amb la demostració de la segona desigualtat ja que

$$[\mathbb{I}_K : K^\times E] = \frac{[\mathbb{I}_{S\cup T} : E]}{[U(S\cup T) : K^\times \cap E]} = \frac{p^{2s}}{p^{s+t}} = p^{s-t} = p^r$$

5.9 Fi de la prova de la llei de reciprocitat

L'objectiu de tota aquesta secció ha estat trobar un homomorfisme entre el grup dels idèles $\mathbb{I}_K$ i el grup de Galois d'una extensió L/K. Aquest morfisme l'hem definit en termes de les lleis de reciprocitat locals en cada plaça,

$$\phi(\mathfrak{d}) = \prod_v \phi_v(a_v).$$

Aquestes aplicacions locals són trivials excepte en un nombre finit de places, per la pròpia definició dels idèles. La llei de reciprocitat també ens diu que aquesta aplicació factoritza pel seu nucli, que és $K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)$. El fet que les normes cauen en el nucli és conseqüència de que ho fa en cadascuna de les places. Ens falta veure que $K^\times$ també ho fa. Això ho veiem en el següent teorema.

Teorema 5.10. 1. Sigui L/K una extensió abeliana finita. Aleshores $\phi_{L/K}(\mathfrak{d}) = 1$ si $\mathfrak{d} \in i(K^\times)$.

2. Sigui L/K una extensió de Galois finita. Aleshores $\sum_v \operatorname{inv}(\alpha) = 0$ per tota $\alpha \in H^2(G, L/K)$.

Demostració. (*de la primera part per una extensió ciclotòmica de* $\mathbb{Q}(\zeta_n)$*:*) Denotarem per σ_n l'automorfisme que envïi l'arrel ζ_m a ζ_m^n. És fàcil veure que n'hi ha prou amb veure el teorema per les arrels l^r-èssimes de la unitat, quan l divideix m, ja que si restringint-nos a aquestes subextensions obtenim el valor 1 per tot l, aleshores tambe valdrà 1 sobre tota l'extensió.
Per a la plaça real infinita, el morfisme d'Artin $\phi_\infty : \mathbb{R}^\times/\operatorname{Nm}(\mathbb{C}^\times) \to \operatorname{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ val $\phi_\infty(a) = \sigma_{\operatorname{sign}(a)}$ on $\operatorname{sign}(a)$ és el signe de a. En la resta, suposem que l'extensió les $\mathbb{Q}(\zeta_{l^r})$ de places finites, tenim que per $a = up^s \in \mathbb{Q}_p^\times$, amb $p \neq l$, p no ramifica per tant l'aplicació d'Artin envia $\phi_p(a) = \sigma_{p^s}$. Quan $p = l$, en canvi, l'aplicació envia $\phi_l(a) = \sigma_{u^{-1}}$ usant els resultats vistos en l'existència de cossos de classe locals. Com que qualsevol nombre racional es pot escriure com a producte de primers enters amb potències enteres llevat d'un signe, n'hi ha prou amb veure que $\phi(a) = 1$, quan $a = -1$, $a = l$ i a és un primer q diferent de l. Usant els valors coneguts de les aplicacions d'Artin locals tenim.

$$\phi_p(-1) = \begin{cases} \sigma_{-1} & \text{si } p = \infty \\ \sigma_{-1} & \text{si } p = l \\ \text{id} & \text{si } p \neq l, \infty. \end{cases}$$

$$\phi_p(l) = \begin{cases} \text{id} & \text{si } p = l \\ \text{id} & \text{si } p \neq l. \end{cases}$$

$$\phi_p(q) = \begin{cases} \sigma_q & \text{si } p = q \\ \sigma_{q^{-1}} & \text{si } p = l \\ \text{id} & \text{si } p \neq l, q. \end{cases}$$

A partir d'aqui és evident veure que $\phi(a) = \prod_p \phi_p(a) = 1$. □

Lema 5.16. Si el punt 1 del teorema 5.10 és cert per una extensió L/K, aleshores també ho és per qualsevol subextensió.

Demostració. Per una extensió intermèdia $K \subset K' \subset L$, l'aplicació d'Artin $\phi_{K'/K}$ és la composició de $\phi_{L/K}$ amb la restricció del grup $\operatorname{Gal}(L/K)$ al grup $\operatorname{Gal}(K'/K)$ prenent només els automorfismes que fixen K'. □

Lema 5.17. Si el punt 1 del teorema 5.10 és cert per una extensió L/K, aleshores també és cert per qualsevol aixecament LK'/K' per K' extensió de K.

Demostració. Fixem la notació dient que $L' = LK'$ i sigui w una plaça de K' per sobre una diferent de v a K. Aleshores tenim un diagrama commutatiu donat per les aplicacions d'Artin.

$$\begin{array}{ccc} K_w'^{\times} & \xrightarrow{\phi_w} & \mathrm{Gal}(L'_w/K'_w) \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle i} \\ K_v^{\times} & \xrightarrow{\phi_v} & \mathrm{Gal}(L_v/K'_v) \end{array}$$

Aquest diagrama es pot transportar als idèles de manera global per obtenir-ne un de la forma següent

$$\begin{array}{ccc} \mathbb{I}'_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow{\scriptstyle \mathrm{Nm}} & & \downarrow{\scriptstyle i} \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

Si el teorema és cert en la part inferior del diagrama, també ha de ser-ho en la superior, donat que tenim una inclusió entre els grups de Galois. □

Lema 5.18. Sigui L/K una extensió abeliana. Si la part 2 del teorema 5.10 és certa, aleshores també ho és la primera. A la inversa, si la part 1 és certa per extensions cícliques, aleshores també ho és la segona.

Lema 5.19. Si la part 2 del teorema 5.10 és certa per a extensions cícliques ciclotòmiques, aleshores també és certa per a qualsevol extensió de Galois finita.

Demostració. Les proves d'aquest teorema recuperen els grups de cohomologia i els productes cup en la successió.

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

Milne, CFT, 8.8. □

Partiem de que la part 1 del teorema era cert per extensions ciclotòmiques de $\mathbb{Q}$. A través del procediment d'aixecament i restricció, veiem que també es dóna la part 1 per a qualsevol extensió ciclotòmica, en particular cíclica. El lema 5.18 ens diu que la part 2 també és certa per aquestes extensions. El lema 5.19 ens diu que la part 2 també serà certa per qualsevol extensió finita de Galois. Finalment, recuperem la part 1 del teorema per a qualsevol extensió tornant al lema 5.18.
Fins aquí arriba la demostració de la llei de reciprocitat d'Artin en la notació idèlica.

5.10 Existència de cossos de classe globals

Un cop vista la reciprocitat en el cas global, volem demostrar el teorema d'existencia, que ens indica que quins subgrups $U \subset \mathbb{I}_K$ és un subgrup de norma per alguna extensió L/K, $U = \mathrm{Nm}\,\mathbb{C}_L$. A diferència del cas local, on obteniem de forma explícita els cossos de classe de tots els subgrups, en aquest cas els cossos de classe seràn una mica més complicats de veure a primera vista, però intentarem fer-ho amb ajuda de la teoria de Kummer, desenvolupada en l'apartat anterior. En aquest cas, no ens podem recolzar sobre cap teoria constructiva com era el cas de Lubin-Tate per als cossos locals.

Lema 5.20. Sigui U un subgrup de norma, i $V \supset U$. Aleshores V també és un subgrup de norma.

Demostració. Prenem L una extensió abeliana tal que $\mathrm{Nm}\,\mathbb{C}_L = U$. Segons la llei de reciprocitat, l'aplicació d'Artin defineix un isomorfisme de la forma

$$\phi : \mathbb{C}_K/U \to \mathrm{Gal}(L/K),$$

de manera que $\phi(V)$ és un subgrup de $\mathrm{Gal}(L/K)$. Podem prendre L' com el cos fix per $\phi(V)$, i ara l'aplicació d'Artin s'escriu com

$$\phi : \mathbb{C}_K/V \to \mathrm{Gal}(L'/K),$$

amb el qual podem tornar a aplicar la llei de reciprocitat i obtenir $\mathrm{Nm}\,\mathbb{C}_{L'} = V$. □

Amb això només hem de demostrar que qualsevol subgrup obert d'índex finit conté algun subgrup de norma. El següent pas és demostrar-ho en el cas que el cos K contingui una arrel p-èssima de la unitat.

Proposició 5.17. Sigui K un cos de nombres que contingui alguna arrel n-èssima de la unitat, i S un conjunt finit de places que contingui les places infinites, tots els primers que divideixen n i prous elements com per que generin el grup de classes (el qual ja hem vist que es pot garantir). Aleshores, qualsevol $a \in K^\times$ tal que a sigui una potència n-èssima a K_v quan $v \in S$ i sigui una unitat quan $v \notin S$, és una potència n-èssima a K.

Demostració. Prenem $L = K[a^{\frac{1}{n}}]$, que és una extensió abeliana sempre que $\zeta_n \in K$. Per hipòtesi, el polinomi $X^n - a$ descompon completament a $K_v[X]$ per tot $v \in S$ i per tant $L_w = K_v$ per totes les $w|v$. Així, l'aplicació norma és exhaustiva. En les altres places $v \notin S$, l'extensió és no ramificada per hipòtesi i per tant l'aplicació norma és exhaustiva sobre les unitats. Aleshores, si $\mathfrak{d} \in \mathbb{I}_S$, també és una norma i

$$K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L) \supset K^\times \mathbb{I}_S = \mathbb{I}_K.$$

Usant la llei de reciprocitat, tenim que l'extensió és trivial, i per tant, a és una potència n-èssima. □

Lema 5.21. Sigui K un cos de nombres que contingui les arrels p-èssimes de la unitat. Aleshores qualsevol subgrup obert $V \subset \mathcal{C}_K$ tal que $\mathcal{C}_K/V$ és d'índex finit d'exponent p és un subgrup de norma: és a dir $V = \operatorname{Nm}_{L/K}(\mathcal{C}_L)$ per alguna extensió finita L/K.

Demostració. Prenem S un conjunt de places finit (en particular, amb s elements) que contingui les places infinites, les places que divideixen p, i suficients primers de manera que $\mathbb{I}_K = K^\times \mathbb{I}_S$. Sigui L l'extensió corresponent a afegir les arrels p-èssimes de $U(S)$, que en particular correspon a l'extensió de Kummer del subgrup $U(S)K^{\times p}$, i sigui

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v.$$

Verificarem que $K^\times E = K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)$. Per això hem de veure que $E \subset \operatorname{Nm}_{L/K}(\mathbb{I}_L)$ i que tenen el mateix índex (que és p^s).
Primer veiem la inclusió. En les places $v \in S$ i $w|v$, la llei de reciprocitat local ens diu que $K_v^\times / \operatorname{Nm}(L_w) \cong \operatorname{Gal}(L_w/K_v)$. Com que l'extensió és d'exponent p, tenim $K_v^{\times p} \subset \operatorname{Nm}_{L/K}(L_w^\times)$. En la resta, l'extensió és no ramificada, i per tant l'aplicació norma és exhaustiva.
Ens falta ara la part de l'índex. Per la llei de reciprocitat global i usant teoria de Kummer,

$$[\mathbb{I}_K : K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)] = [L : K] = [U(S)K^{\times p} : K^{\times p}] = [U(S) : U(S) \cap K^{\times p}] = [U(S) : U(S)^p] = p^s,$$

on al final hem tornat a usar el teorema de les unitats de Dirichlet.
Altrament,

$$[\mathbb{I}_K : K^\times E] = [\mathbb{I}_S K^\times : E K^\times] = \frac{[\mathbb{I}_S : E]}{[\mathbb{I}_S \cap K^\times : E \cap K^\times]} = \frac{p^{2s}}{p^s} = p^s,$$

on al final hem usat els resultats finals de la segona desigualtat.
Un cop hem verificat que $K^\times E = K^\times \operatorname{Nm}_{L/K}(\mathbb{I}_L)$, prenem $V \subset \mathcal{C}_K$ tal que $\mathcal{C}_K/V$ és d'exponent p. Podem prendre U que sigui l'antiimatge de V per la inclusió $i : \mathbb{I}_K \to \mathcal{C}_K$, tenint $\mathbb{I}_K/U$ també exponent p. Com que U és obert, $U \supset \prod_{v \in S} 1 \times \prod_{v \notin S} U_v$, i com a tal $U \supset \mathbb{I}_K^p$. En particular, $U \supset EK^\times$ i com que ja hem demostrat que $EK^\times/K^\times$ és un subgrup de norma i que qualsevol subgrup que contingui un de norma també ho és, ja queda provat el resultat. □

Per acabar de demostrar el teorema, haurem de suposar cert el teorema de limitació de la norma que ja hem vist per a extensions locals.

Teorema 5.11. Sigui M/K una extensió de cossos globals, no necessàriament abeliana. Sigui L/K la subextensió abeliana maximal. Aleshores,

$$\operatorname{Nm}_{M/K}(\mathcal{C}_M) = \operatorname{Nm}_{L/K}(\mathcal{C}_L).$$

Això es demostra de manera similar al cas local.

Lema 5.22. Sigui $U \subset \mathcal{C}_K$ un subgrup obert d'index finit. Si existeix una extensió K'/K (no necessàriament abeliana) tal que $\mathrm{Nm}^{-1}_{K'/K}(U)$ és un subgrup de norma de $\mathcal{C}_{K'}$, aleshores també ho és U.

Demostració. Sigui $U' = \mathrm{Nm}^{-1}_{K'/K}(U)$ i sigui L una extensió abeliana de K' tal que $\mathrm{Nm}_{L/K}(\mathcal{C}_L) = U'$. Prenem M la subextensió abeliana més gran continguda a L/K. Usant el teorema de limitació de la norma tenim

$$\mathrm{Nm}_{M/K}(\mathcal{C}_M) = \mathrm{Nm}_{L/K}(\mathcal{C}_L) = \mathrm{Nm}_{K'/K}(\mathrm{Nm}_{L/K'}(\mathcal{C}_L)) = \mathrm{Nm}_{K'/K}(U') \subset U$$

Amb això ja tenim que U també és un subgrup de norma. □

Teorema 5.12. Un subghrup $U \subset \mathcal{C}_K$ és de norma, si i només si, és obert i d'índex finit.

Demostració. En una implicació, usem la llei de reciprocitat quadràtica per veure que els subgrups de norma són d'índex finit i oberts.
En l'altra, ho provem per inducció sobre l'índex de U. Si és trivial, no tenim res a demostrar. En cas contrari, existeix algun p dividint l'índex $[\mathcal{C}_K : U]$. Usant el teorema anterior, podem suposar que K conté una arrel p-èssima de la unitat. Amb això, podem prendre un subgrup intermedi d'índex p, $U \subset U_1 \subset \mathcal{C}_K$. Per aquest subgrup, podem aplicar el lema 5.14 per trobar una extensió K'/K tal que $\mathrm{Nm}_{K'/K}(\mathcal{C}_{K'}) = U_1$. En particular, una extensió abeliana i de grau p és cíclica. Prenem ara $U' = \mathrm{Nm}_{K'/K}(U)$. L'aplicació norma en aquesta extensió pren la forma

$$\mathrm{Nm}_{K'/K} : \mathcal{C}_{K'} \to \mathcal{C}_K/U,$$

i té imatge U_1/U i nucli U'. Aleshores, podem veure els índex a través del primer teorema d'isomorfisme

$$[\mathcal{C}_{K'} : U'] = [U_1 : U] = \frac{[\mathcal{C}_K : U]}{[\mathcal{C}_K : U_1]} = \frac{[\mathcal{C}_K : U]}{p}.$$

Per inducció, U' és un subgrup de norma, i pel lema anterior U també ho és. □

Aquest resultat ja val per a demostrar el teorema d'existència en termes de idèles. Desafortunadament, aquest procediment de demostració no és constructiu com sí que era el cas local i ens hauriem de buscar un altre procediment per a poder construir els cossos de classe.

6 Aplicacions i altres resultats relacionats

El propòsit d'aquesta secció és, un cop provats els resultats de la teoria de cossos de classe globals, trobar algunes aplicacions senzilles dels teoremes, així com presentar el teorema de Chebotarev, que està íntimament relacionat amb els resultats estudiats. Aquesta secció hauria de servir per destacar la centralitat de la teoria de cossos de classe dins l'estudi de la teoria de nombres, essent una magnifica eina per a classificar les extensions d'un cos donat. Per tant, es presenten diversos àmbits d'estudi que sorgeixen a partir d'aquesta teoria, o en tot cas donen peu a problemes relacionats. Alguns d'ells són problemes encara oberts, d'altres són previs al desenvolupament que hem presentat. Tots ells, són mostrats de manera resumida a mode de conclusió (o semiconclusió) del treball per tal fer explícita la necessitat de seguir llegint sobre aquestes questions.

6.1 El cos de classe de Hilbert

Com a conseqüència del teorema d'existència, sabem que donat un modulus i un subgrup del seu grup de classe, podem construir una extensió de manera que al fer quocient per aquest subgrup, l'aplicació d'Artin esdevingui un isomorfisme. Si prenem com a subgrup de congruència els ideals principals i el modulus trivial $\mathfrak{m} = 1$, tenim un isomorfisme

$$C_K = \frac{I_K}{P_K} \cong \mathrm{Gal}(L/K)$$

per alguna extensió L/K. Podem comprovar que aquesta extensió coincideix amb el cos de classes de Hilbert, com hem mencionat abans.

Proposició 6.1. El grup de Galois del cos de classes de Hilbert és isomorf al grup de classes.

Demostració. Si $\mathfrak{m} = 1$, aleshores $I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$ és el grup de classes, i sabem que cap dels primers ramificarà perquè haurien de dividir $\mathfrak{m}$. Sigui M una altra extensió no ramificada; alehsores el modulus corresponent pel teorema d'existència és $\mathfrak{m} = 1$. Per tant,

$$P_K = i(K)\,\mathrm{Nm}_{L/K}(I_L) \subset i(K)\,\mathrm{Nm}_{M/K}(I_M),$$

que alhora son els nuclis de l'aplicació d'Artin. Pel corol·lari 5.1, això implica $M \subset L$. □

Això ens permet construir explícitament alguns cossos de classe de Hilbert.

Exemple 6.1. Per a $K = \mathbb{Q}$, el grup de classes és trivial ja que tots els ideals fraccionaris són principals i per tant el cos de classes de Hilbert és ell mateix. Això coincideix amb el que hem vist al teorema 1.6, que assegura que en qualsevol extensió de $\mathbb{Q}$ ramifica algun primer.

Per a extensions quadràtiques en que el grup de classes no sigui trivial, un resultat útil pot trobar el cos de classes de Hilbert en alguns casos és el següent lema.

Lema 6.1. Sigui $L = K(\sqrt{u})$ una extensió quadràtica i $u \in \mathcal{O}_K$. Sigui $\mathfrak{p}$ un primer de $\mathcal{O}_K$.

1. Si $2u \notin \mathfrak{p}$, aleshores $\mathfrak{p}$ no ramifica a L.
2. Si $2 \in \mathfrak{p}$ i $u = b^2 - 4c$, per algun $b, c \in \mathcal{O}_K$, aleshores $\mathfrak{p}$ no ramifica a L.

Demostració. Per a la primera pat, n'hi ha prou amb veure que el discriminant de l'extensió és $4u$, al qual $\mathfrak{p}$ no divideix i per tant $\mathfrak{p}$ no ramifica. Per a la segona, escrivim l'extensió com $K(\frac{-b+\sqrt{u}}{2})$ on estem afegint una arrel del polinomi $X^2 + bX + c$. Això implica que el seu discriminant $b^2 - 4c = u \in \mathfrak{p}$. Per la mateixa raó, aquest polinomi no pot ramificar. □

Exemple 6.2. Usant la fita de Minkowski, podem veure que el grup de classes de $K = \mathbb{Q}(\sqrt{-5})$ té 2 elements. Per tant, trobar el cos de classes de Hilbert consisteix a trobar una extensió quadràtica no ramificada de K. Aquesta és $K(\sqrt{-1})$. Això es deu a que només poden ramifcar els ideals que ho facin a $\mathbb{Q}(\sqrt{-1}, \sqrt{-5})$ que són 2 i 5. Per veure que 2 no ramifica, usem la segona part del lema, ja que $2 \in (2)$, $-1 \notin (2)$ i $-1 = (\sqrt{-5})^2 - 4(-1)$. Per veure que $\sqrt{-5}$ no ramifica usem la primera part i veiem que $-2 \in (\sqrt{-5})$.

Exemple 6.3. Usant la fita de Minkowski es pot veure que el grup de classes de $K = \mathbb{Q}(\sqrt{-14})$ és d'ordre 4. Demostrarem que el seu cos de classe de Hilbert és $K(\sqrt{2\sqrt{2}-1})$. Per veure-ho, construirem una extensió intermèdia $K_1 = K(\sqrt{2})$ i provarem que K_1/K i $K(\sqrt{2\sqrt{2}-1})/K_1$ són extensions no ramificades.

1. $K(\sqrt{2})/K$ és no ramificada. Si $2 \notin \mathfrak{p}$, aleshores pel lema anterior, $\mathfrak{p}$ no ramifica. Falta veure el cas $2 \in \mathfrak{p}$. Com que $\sqrt{-14} \in K$ i $\sqrt{2} \in K_1$, aleshores $\sqrt{-7} \in K_1$. En aquest ideal, tenim $-7 \notin \mathfrak{p}$ i podem escriure $-7 = 1^2 - 4 \cdot 2$, el ual ens dóna que $\mathfrak{p}$ no ramifica per la segona part del lema.

2. Prenem $L = K_1(\sqrt{\alpha})$ on $\alpha = 2\sqrt{2} - 1$. Si prenem un altre element $\alpha' = -2\sqrt{2} - 1$, es pot veure que $\sqrt{\alpha\alpha'} = \sqrt{-7} \in K_1$. Per tant, $\sqrt{\alpha'} \in L$. Sigui $\mathfrak{p}$ un primer de K_1. Si $2 \notin \mathfrak{p}$, com que $\alpha + \alpha' = -2$, algun α, α' no està en l'ideal, per tant podem aplicar la primera part del lema. Si $2 \in \mathfrak{p}$, aleshores $\alpha \notin \mathfrak{p}$ ja que té la forma $\alpha = 2\sqrt{2} - 1$. Per tant, apliquem la segona part del lema basant-nos en la igualtat $\alpha = (1 + \sqrt{2})^2 - 4$.

Els cossos de nombres quadràtics donen lloc a nombrosos problemes de gran interès, segurament motivats per la seva simplicitat, i una pregunta natural és tractar de determinar per a quins d el cos $\mathbb{Q}(\sqrt{-d})$ té nombre de classes 1. Gauss es va a adonar de que quan

$$d = 1, 2, 3, 7, 11, 19, 43, 67, 163$$

aquesta propietat es satisfà, però no seria fins l'any 1960 quan es va provar que aquests eren els únics cossos quadràtics imaginaris amb cos de classes de Hilbert trivial.
En el cas de cossos quadràtics reals això és encara una pregunta oberta, i no es sap si el nombre de cossos quadràtics reals amb grup de classes trivial és finit o infinit. Aquestes diferències entre cossos quadràtics imaginaris i reals també la trobem quan intentem generalitzar el teorema de Kronecker-Weber i trobar l'extensió abeliana maximal d'un cos de nombres quadràtic.
Suposi's que K és un cos quadràtic amb grup de classes trivial. Aleshores, la seva extensió abeliana maximal es construeix afegint les coordenades dels punts de torsió d'una corba el·líptica amb multiplicació complexa per l'anell d'enters del cos. Tot i que ometrem les definicions i el desenvolupament d'aquesta idea, ho il·lustrarem amb un exemple. Sigui $K = \mathbb{Q}(\sqrt{-1})$; una corba el·líptica amb multiplicació complexa pels enters gaussians és aquella en la qual el reticle associat admet la multiplicació per i com un endomorfisme, per exemple

$$y^2 = x^3 - x.$$

La n-torsió d'aquesta corba serà un grup isomorf a $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ i les coordenades d'aquests punts estaran definides sobre extensions abelianes de K. Així, la composició de totes aquestes extensions genera l'extensió abeliana maximal, donant una analogia interessant amb el teorema de Kronecker-Weber, que coincideix amb la noció de Lubin-Tate, que hem usat al capítol 4: afegir punts de torsió de grups formals, en aquest cas, corbes el·líptiques. En el cas dels racionals, l'extensió abeliana maximal es construeix afegint la torsió del la circumferència, el qual sembla evident ja que les extensions ciclotòmiques es construeixen afegint punts de la circumferència.
Noti's que si el nombre de classes no és trivial aquesta idea requereix una petita observació: la torsió de la corba el·líptica genera extensions abelianes del cos de classes de Hilbert de K, i no del propi cos; en qualsevol cas, la construcció del cos de classes de Hilbert general en aquest cas és força senzilla, un cop coneguda la relació amb la teoria de corbes el·líptiques: n'hi ha prou amb adjuntar a K l'anomenat invariant j de la corba el·líptica, una funció modular que mesura en un sentit adient classes d'isomorfismes de corbes el·líptiques. Aquest invariant j és un enter algebraic que pertany a $\mathbb{Z}$ quan el cos quadràtic imaginari té nombre de classes 1. Això dóna una explicació del conegut fet de que el nombre $e^{\pi\sqrt{163}}$ sembli un enter racional.
En el cas que s'ha comentat amb anterioritat de $K = \mathbb{Q}(\sqrt{-14})$, es té que

$$j = 8 \cdot \left(323 + 228\sqrt{2} + (231 + 161\sqrt{2})\sqrt{2\sqrt{2}-1}\right)^3.$$

Estendre la teoria de la multiplicació complexa al cas quadràtic real és un dels reptes de la recerca en teoria de nombres avui en dia. Per exemple, Henri Darmon ha intentat donar una resposta a aquesta qüestió introduint els anomenats punts de Stark-Heegner (substituts p-àdics dels punts de Heegner que apareixen en la teoria de la multiplicació complexa), o més recentment el mateix Darmon juntament amb Jan Vonk amb proposat una construcció conjectural basada en el que s'anomena "singular moduli".

Idènticament a la construcció feta per al Hilbert class field, es pot construir una extensió que correspongui al subgrup d'ideals principals $i(K_{\mathfrak{m},1})$ d'un modulus $\mathfrak{m}$ al que podem anomenar cos de classes radial. Això ho farem servir quan vulguem permetre que uns quants primers sí que ramifiquin.

Exemple 6.4. En el cas d'un modulus $\mathfrak{m} = m\infty$, el cos de classes radial serà el cos ciclotòmic $\mathbb{Q}(\zeta_m)$.

6.2 El teorema de Chebotarev

EL teorema de Chebotarev proporciona informació rellevant sobre la proporció de nombres primers complint una certa propietat en una extensió de cossos globals. En el desenolupament clàssic de la teoria de cossos de classes, aquest teorema és una eina per demostrar l'exhaustivitat de l'aplicació d'Artin. Aquí, veurem quines conseqüències podem deduir d'ell un cop demostrada la llei de recirocitat. Denotarem per $\mathbb{P}_K$ al conjunt de tots els primers de K.

Definició 6.1. Sigui $S \subset \mathbb{P}_K$ un conjunt de primers finits en un cos K. La densitat de Dirichlet es defineix com

$$\delta(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{-\log(s-1)},$$

sempre que aquest limit existeixi.

Aquesta definició compleix aquelles propietats esperables d'una densitat en un conjunt de cardinal infinit numerable.

Proposició 6.2.

1. $\delta(\mathbb{P}_K) = 1$.
2. Si $S \subset T$, i els dos densitats existeixen, aleshores, $\delta(S) \leq \delta(T)$.
3. Si la densitat d'un conjunt S existeix, aleshores $0 \leq \delta(S) \leq 1$.
4. Si S, T són dos conjunts disjunts, aleshores $\delta(S \cup T) = \delta(S) + \delta(T)$.
5. Si S és finit, aleshores $\delta(S) = 0$.
6. Si S, T difereixen d'un nombre finit d'elements, aleshores $\delta(S) = \delta(T)$.

El que volem és usar aquesta definició per a estudiar les propietats de densitat de nombres primers en un cos global. Per exemple, si prenem una extensió L/K no necessàriament abeliana, donat $\mathfrak{p}$ un primer no ramificat, sabem per la proposició 1.2 que els elements $\left(\frac{\mathfrak{P}}{L/K}\right)$ per $\mathfrak{P}$ primers per sobre de $\mathfrak{p}$ són tots conjugats. El teorema de Chebotarev ens dóna la densitat d'aquestes classes de conjugació.

Teorema 6.1. (*Chebotarev*) Sigui L/K una extensió de Galois, i sigui $[\tau] = \{\sigma^{-1}\tau\sigma\, \sigma \in \mathrm{Gal}(L/K)\}$ la classe de conjugació d'un element $\tau \in \mathrm{Gal}(L/K)$. Aleshores el conjunt

$$S = \{\, \mathfrak{p} \in \mathbb{P}_K \text{ tal que } \mathfrak{p} \text{ no ramificat } i \left(\frac{\mathfrak{P}}{L/K}\right) \in \langle\tau\rangle \ \forall \mathfrak{P} | \mathfrak{p} \,\}$$

té densitat de Dirichlet

$$\delta(S) = \frac{|\,\langle\tau\rangle\,|}{[L:K]}$$

Durant tot el treball hem evitat l'ús de les sèries L. Tot i així, no s'ha trobat encara cap demostració d'aquest teorema que no usi mètodes analítics. Tot i així, les conseqüencies d'aquest teorema abarquen resultats molt interessants.

Corol·lari 6.1. Sigui L/K una extensió abeliana i $\mathfrak{m}$ un modulus divisible per tots els primers que ramifiquen a L. Aleshores, donat $\sigma \in \mathrm{Gal}(L/K)$, el conjunt de primers que no divideixen $\mathfrak{m}$ i compleixen $\left(\frac{\mathfrak{P}}{L/K}\right) = \sigma$ té densitat $\frac{1}{[L:K]}$, i per tant, és infinit.

Demostració. En el cas que l'extensió sigui abeliana, la classe de conjugació de σ només conté l'element σ i per tant té cardinal 1. □

Això ens demostra que l'aplicació d'Artin és exhaustiva, però a més ens dóna informació addicional. Donat un element del grup de Galois $\mathrm{Gal}(L/K)$, existeixen infinits primers que van a ell per l'aplicació d'Artin prenent un modulus $\mathfrak{m}$. Una altra conseqüència rellevant del teorema de Chebotarev és el teorema de la progressió aritmètica de Dirichlet, quan L és una extensió ciclotòmica.

Teorema 6.2. (*de la progressió aritmètica de Dirichlet*) Siguin $a, n \in \mathbb{Z}$ dos enters positius primers entre si, aleshores existeixen infinits primers $p \in \mathbb{Z}$ de la forma $p = a + kn$. En particular tenen densitat $\frac{1}{\phi(n)}$.

Demostració. Prenem $L = \mathbb{Q}(\zeta_n)$ la n-èssima extensió ciclotòmica. El seu grup de Galois s'identifica amb $(\mathbb{Z}/n\mathbb{Z})^\times$. En particular s'identifica enviant a al morifsme $\sigma(\zeta_n) = \zeta_n^a$. Prenem ara un primer $p \in \mathbb{Z}$ que no divideixi n i per tant no ramifiqui a L. Prenem també un altre $\mathfrak{P} \subset \mathcal{O}_L$ per sobre seu amb un $\sigma \in \mathrm{Gal}(L/K)$ que actuï com el Frobenius a $\mathfrak{P}$. Aleshores, com que $\mathrm{Nm}(p\mathbb{Z}) = p$, σ actúa de la manera $\sigma(\zeta_n) = \zeta_n^p$. Pel teorema de Chevotarev, donat un $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, existeixen infinits primers que com l'anterior que van a aquest element del grup de Galois. En particular, aquests primers compliràn $p = a \mod n$. També sabem que el grau de l'extensió és $\phi(n)$, el qual ens dóna la densitat de la classe de conjugació. □

6.3 Generalització de les lleis de reciprocitat

La finalitat d'aquesta secció és recuperar les lleis de reciprocitat, com per exemple, la reciprocitat quadràtica de Gauss, presentada a la secció introductòria, a partir de la reciprocitat d'Artin.
Els cossos amb els que tractarem seran cossos de la forma $K(\sqrt[n]{\alpha})$ amb $\alpha \in \mathcal{O}_K$ i K una extensió de $\mathbb{Q}$ que contingui les arrels n-èssimes de la unitat. Això garanteix que l'extensió $K(\sqrt[n]{\alpha})/K$ és de Galois. També sabem que aquesta extensió té grup de Galois contingut a $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, ja que tot element $\sigma \in \mathrm{Gal}(K(\sqrt[n]{\alpha})/K)$ actua de la forma $\sigma(\sqrt[n]{\alpha}) = \zeta_n \sqrt[n]{\alpha}$, per alguna arrel n-èssima primitiva de la unitat ζ_n. Fixarem aquesta arrel primitiva a partir d'ara.
El primer objectiu es generalitzar el símbol de Legendre a un cos d'aquest tipus. Per fer això, requerim primer generalitzar el teorema petit de Fermat. Fixem la notació com $\mathfrak{p} \subset \mathcal{O}_K$ un primer de K, i $k = \mathcal{O}_K/\mathfrak{p}$ el cos residual que té $N(\mathfrak{p})$, que sigui coprimer amb n. Prenem també $\alpha \in \mathcal{O}_K$ que no estigui a $\mathfrak{p}$, que farem coincidir amb el α anterior.

Teorema 6.3. (*Teorema petit de Fermat generalitzat*) En les condicions definides anteriorment

$$\alpha^{N(\mathfrak{p})-1} \equiv 1 \mod \mathfrak{p}$$

Demostració. Aquest teorema es pot demostrar de manera senzilla coneixent el teorema de Legendre, que diu que els ordres dels elements d'un grup divideixen l'ordre del grup, aplicat al grup multiplicatiu de $\mathcal{O}_K/\mathfrak{p}$ que té ordre $N(\mathfrak{p}) - 1$. Altrament, podem prendre la mateixa idea que en el teorema petit clàssic. Siguin (a_i) un conjunt de representants de les classes no trivials de k, que n'hi ha $N(\mathfrak{p}) - 1$, aleshores, donat que $\overline{\alpha}$ no defineix la classe trivial, (αa_i) també defineix un conjunt de classes no trivials. Els productes d'ambdues seran iguals a k.

$$\prod_i a_i = \prod \alpha a_i = \alpha^{N(\mathfrak{p})-1} \prod_i a_i$$

Com que la igualtat es dóna modul $\mathfrak{p}$, podem concloure que

$$\alpha^{N(\mathfrak{p})-1} \cong 1 \mod \mathfrak{p}.$$

□

Teorema 6.4. Sota les condicions anteriors, $X^n - 1$ és un polinomi separable a K, n divideix $N(\mathfrak{p}) - 1$ per tot primer de K i per tant existeix una única arrel n-èssima de la unitat (que escriurem com ζ_n^s) tal que

$$\alpha^{\frac{N(\mathfrak{p})-1}{n}} \cong \zeta_n^s \mod \mathfrak{p}$$

Demostració. L'extensió de Galois del polinomi $X^n - 1$ sobre $\mathbb{Q}$ estarà continguda en K. Per tant, serà un polinomi separable dins d'aquesta extensió (ja que la seva derivada nX^{n-1} és un polinomi no nul mòdul $\mathfrak{p}$, ja que n ho és). Això ens permet afirmar que $1, \zeta_n, \ldots, \zeta^{n-1}$ són totes arrels diferents, també mòdul $\mathfrak{p}$.
Definim a $k^\times$ el morfisme $f : k^\times \to k^\times$ definida per $f(u) = u^n$ té per nucli les arrels de la unitat. Per tant,

usant el teorema d'isomorfisme, el nucli de l'aplicació té n elements, i la imatge $\frac{N(\mathfrak{p})-1}{n}$ elements, el qual demostra la divisibilitat. Així, podem construir un altre morfisme $g : k^\times \to k^\times$ definit com $g(u) = u^{\frac{N(\mathfrak{p})-1}{n}}$, que té per imatge les arrels de la unitat, dualment al morfisme anterior. Aleshores, per tot element $\alpha \notin \mathfrak{p}$, $\alpha^{\frac{N(\mathfrak{p})-1}{n}}$ és a la mateixa classe que una única arrel mòdul $\mathfrak{p}$. □

Definició 6.2. A l'arrel n-èssima definida en el teorema anterior l'anomenarem símbol de Legendre n-èssim, o símbol de residu-potència. El denotarem per

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n$$

.

Definició 6.3. Sigui $\mathfrak{a}$ un ideal de $\mathcal{O}_K$ que descompon en en ideals primers com $\mathfrak{p}_i^{m_i} \dots \mathfrak{p}_s^{m_s}$, i prenem $\alpha \notin \mathfrak{a}$ i $n \in \mathbb{Z}$ coprimer amb $\mathfrak{a}$ també. Aleshores podem definir

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n = \prod_i \left(\frac{\alpha}{\mathfrak{p}_i}\right)_n^{m_i}$$

Alhora, si $\mathfrak{m}$ és un modulus que contingui els primers que divideixin $n\alpha$, aquesta definició indueix un morfisme

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K^{S(\mathfrak{m})} \to \mu_n$$

on μ_n és el grup d'arrels n-èssimes de la unitat, que és isomorf a $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times$.

El nostre objectiu és arribar a recuperar la llei de reciprocitat quadràtica, però abans demostrarem una llei de reciprocitat que valgui per a les extensions $K(\sqrt[n]{\alpha})/K$ amb les que hem tractat, de les quals la quadràtica només és un cas particular. Totes elles es poden demostrar com a conseqüència de la llei de reciprocitat d'Artin.

Teorema 6.5. (*de reciprocitat dèbil*) Sigui K un cos de nombres que contingui les arrels n-èssimes de la unitat i $L = K(\sqrt[n]{\alpha})$ amb $\alpha \in \mathcal{O}_K$ l'extensió amb la que hem estat treballant. Prenem també $\mathfrak{m}$ un modulus divisible per tots els primers que divideixen $n\alpha$ i assumim que $\mathrm{Ker}(\hat{\Psi}_{L/K})$ és un subgrup de congruència. Aleshores, el següent diagrama és commutatiu

$$\begin{array}{ccc} I_K^{S(\mathfrak{m})} & \xrightarrow{\hat{\Psi}_{L/K'}} & \mathrm{Gal}(L/K) \\ & \searrow^{\left(\frac{\alpha}{\cdot}\right)_n} & \downarrow i \\ & & \mu_n \end{array}$$

Donat que el nucli és un subgrup de congruència (conté $i(K_{\mathfrak{m},1})$), aquest diagrama indueix un morfisme exhaustiu:

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \to G \subset \mu_n$$

on G és la imatge de $\mathrm{Gal}(L/K)$ dins de μ_n.

Demostració. Donat $\mathfrak{p} \in I_K^{S(\mathfrak{m})}$, hem de veure que $\hat{\Psi}_{L/K}(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\cdot}\right)_n (\sqrt[n]{\alpha})$, ja que $\sqrt[n]{\alpha}$ és un generador de l'extensió. Per la definició de l'aplicació d'Artin sabem que això equival a veure

$$\left(\frac{\mathfrak{p}}{L/K}\right)(\sqrt[n]{\alpha}) = \left(\frac{\alpha}{\mathfrak{p}}\right)_n (\sqrt[n]{\alpha}).$$

Recordem que per la definició de l'element $\left(\frac{\mathfrak{p}}{L/K}\right)$, aquest actúa enviant

$$\left(\frac{\mathfrak{p}}{L/K}\right)(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha}^{N(\mathfrak{p})} \mod \mathfrak{p}$$

i dividint per l'element $\sqrt[n]{\alpha}$ obtenim

$$\frac{\left(\frac{\mathfrak{p}}{L/K}\right)(\sqrt[n]{\alpha})}{\sqrt[n]{\alpha}} = \sqrt[n]{\alpha}^{N(\mathfrak{p})-1} = \left(\frac{\alpha}{\mathfrak{p}}\right)_n \mod \mathfrak{p}$$

Però, com que l'element pertany a $D_\mathfrak{p}$ aquesta igualtat a k també ho és a K. Tot això ho podem fer ja que l'extensió L/K és no ramificada sempre que n i $\mathfrak{p}$ siguin coprimers.
Donat que l'aplicació d'Artin és exhaustiva i que estem suposant que $i(K_{\mathfrak{m},1}) \subset \operatorname{Ker}(\hat{\Psi}_{L/K}) \subset I_K^{S(\mathfrak{m})}$, el símbol de Legendre esdevé una aplicació

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}) \to I_K^{S(\mathfrak{m})}/\operatorname{Ker}(\hat{\Psi}_{L/K}) \twoheadrightarrow G \subset \mu_n$$

□

Corol·lari 6.2. (reciprocitat quadràtica) Siguin p, q primers imparells diferents. Aleshores,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Demostració. A la secció introductòria ja haviem vist que això equival a veure

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right)$$

on $p^* = (-1)^{\frac{p-1}{2}}p$.
És senzill veure, usant els ressorts de la teoria de Galois, que la única subextensió quadràtica de $\mathbb{Q}(\zeta_p)$ és $\mathbb{Q}(p^*)$. En l'exemple 5.2 hem vist com s'aplica la reciprocitat d'Artin sobre l'extensió $\mathbb{Q}(\zeta_p)$ usant el modulus $\mathfrak{m} = p\infty$, i $\operatorname{Ker}\hat{\Psi}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}} = i(K_{\mathfrak{m},1})$, per tant el grup de Galois és isomorf al grup de classes de modulus i ademés el nucli és un subgrup de congruència. Es pot demostrar que això també val per qualsevol subextensió, per exemple per $\operatorname{Ker}\hat{\Psi}_{\mathbb{Q}(p^*)/\mathbb{Q}}$.
La llei de reciprocitat dèbil ens indica, doncs, que tenim un morfisme exhaustiu

$$\left(\frac{p^*}{\cdot}\right)_2 : I_\mathbb{Q}^{S(\mathfrak{m})}/i(\mathbb{Q}_{\mathfrak{m},1}) \twoheadrightarrow \operatorname{Gal}(\mathbb{Q}(p^*)/\mathbb{Q}) = \{\pm 1\}$$

Aquesta mateixa aplicació la podem composar amb la aplicació que envia $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ a l'ideal $a\mathbb{Z} \in I_\mathbb{Q}^{S(\mathfrak{m})}/i(\mathbb{Q}_{\mathfrak{m},1})$, que induirà un isomorfisme. Aleshores, al composar aquests dos morfismes ens apareix un nou morfisme

$$\left(\frac{p^*}{\cdot}\right) : \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \to \{\pm 1\}$$

Però com que ambdós grups són cíclics, la teoria de grups ens indica que només hi ha un morifsme no trivial d'aquest tipus. Tal i com havíem definit el símbol de Legendre a la primera secció, aquest també és un morfisme no trivial entre aquests dos grups

$$\left(\frac{\cdot}{p}\right) : \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \to \{\pm 1\}$$

Això implica que les dues aplicacions són iguals.

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$$

□

6.4 Generalitzacions de la teoria de cossos de classe

Durant tot el treball, hem descrit els elements de Frobenius $\left(\frac{p}{E/\mathbb{Q}}\right)$, per a una extensió dels racionals $E/\mathbb{Q}$. La teoria de cossos de classe ens ha permès descirure aquests elements en el cas que l'extensió sigui abeliana. La pregunta que sorgeix de manera natural és com generalitzar aquests resultats per a extensions no necessàriament abelianes. Per això cal introduir la noció de representació d'un grup G sobre un espai vectorial V, com un morfisme $\rho : G \to \mathrm{GL}(V)$ que ens permet veure el grup com a automorfismes de V.
Implícitament, hem estat fent això per a les extensions de $\mathbb{Q}$, ja que qualsevol morfisme $\sigma : G \to \mathbb{C}^\times$, el podem pensar com un caràcter de Dirichlet $\chi_\sigma : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ per algun $N > 0$, de manera que $\sigma(\left(\frac{p}{E/\mathbb{Q}}\right)) = \chi_\sigma(p)$ per a tot primer p no ramificat en E. Això es pot garantir gracies al teorema de Kronecker-Weber, ja que ens premet garantir que el grup G conté algun subgrup de la forma $(\mathbb{Z}/N\mathbb{Z})^\times$ al estar E continguda en algún cos ciclotòmic $\mathbb{Q}(\zeta_N)$. Donat que $GL(\mathbb{C}) \cong \mathbb{C}^\times$, els caràcters de Dirichlet es poden pensar com representacions de $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ sobre l'espai vectorial unidimensional $\mathbb{C}$. Per tant, les extensions abelianes corresponen a les representacions unidimensionals.
El prpòsit de les conjectures proposades per Robert Langlands és generalitzar aquesta ideal de les representacions dimensió $n \geq 2$ de la forma $\sigma : \mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$, quan l'extensió amb la que tractem no és abeliana. D'aquesta manera, reduïm el problema a estudiar els elements $\{\sigma(\mathrm{Frob}_p)\}$ llevat de conjugació. Una primera aproximació és estudiar el polinomi característic els endomorfismes corresponents

$$\det(\mathrm{id}_n - \sigma(\mathrm{Frob}_p)p^{-s}),$$

i per això s'introdueix l'anomenada sèrie L de Dirichlet

$$L(s,\sigma) = \prod_p \Big(\det(\mathrm{id}_n - \sigma(\mathrm{Frob}_p)p^{-s}) \Big)^{-1};$$

que generalitza les series habituals comentades en la secció introductòria per als caràcters de Dirichlet. La definició donada no és del tot correcta ja que s'ha d'incloure una petita modificació pel que fa els primers que ramifiquen.
Per a una extensió arbitrària E i una σ donada, Artin derivà algunes propietats analítiques de $L(s,\sigma)$, però no descobrí l'anàleg apropiat dels caràcters de Dirichlet en el cas de dimensió 1. Anys més tard, Langlands aïllà la noció de representació automorfa per al grup GL_n sobre els adèles de $\mathbb{Q}$, usant la teoria de formes modulars. *Dietmar, AF.* A més, associà funcions L amb aquestes representacions automorfes, generalitzant així la noció de funció L de Dirichlet. Finalment, ell conjecturà que cada representació n-dimensional d'Artin σ (amb sèrie associada $L(s,\sigma)$) es correspon amb una representació automorfa π_σ de GL_n amb la mateixa sèrie L, que denotem $L(s,\pi_\sigma)$.
Però les conjectures proposades per Langlands es proposen anar una mica més enllà: un dels seus objectius era també relacionar objectes de naturalesa geomètrica (motius associats a varietats algebraiques), aritmètica (representacions de Galois) i de teoria de representacions (formes automorfes). Les funcions L actuen com a lligam entre aquests objectes, i la geometria algebraica juga un paper central. Un exemple clàssic ho veiem a la conjectura de modularitat que va permetre provar l'últim teorema de Fermat: per una banda tenim un objecte automorf (una forma modular), i aquest es correspon de forma natural amb un objecte geomètric (una varietat abeliana, que és una corba el·líptica en el cas de que la forma modular tingui coeficients racionals) i al mateix temps tenim una representació de Galois associada a aquests objectes. El gran resultat de Wiles, Taylor-Wiles i després Breuil-Conrad-Diamond-Taylor va ser el veure que tota corba el·líptica és modular, és a dir, té associada una forma automorfa. En aquesta direcció, un altre problema obert és l'anomenada conjectura de Fontaine-Mazur. Suposi's donada una representació

$$\rho : G_\mathbb{Q} \to \mathrm{GL}(V)$$

irreductible (amb cap subrepresentació pròpia $\rho_{|W}$, per un subespai W) i l-àdica (sobre $\mathbb{Q}_l$), que ramifica només en un nombre finit de places, i de manera que $\rho|_{G_{\mathbb{Q}_l}}$ i complint unes certes condicions tècniques. Llavors, el que afirma és que existeix una varietat projectiva i llisa $X/\mathbb{Q}$ de manera que V és un subquocient d'un cert grup de cohomologia de la varietat. Tots els resultats oberts que he presentat, que suposen direccions importants en la teoria moderna de nombres, permeten veure la centralitat dels resultats que hem demostrat tant per les seves implicacions dins la teoria de cossos com les conseqüències geomètriques de tots ells.

7 Bibliografia

1. Brown, J.L., *Local class field theory*, Disponible a cecas.clemson.edu/ jimlb/CourseNotes/localcft.pdf, Pasadena, 2008.
2. Cassels, J.W.S., Frohlich, A., *Algebraic number theory*, Thompson book company, Washington D.C., 1967.
3. Cox, D., *Primes of the form* $x^2 + ny^2$, John Wiley and sons, Amherst, 1989.
4. Deitmar, A., *Automorphic forms*, Springer, Tübingen, 2010.
5. Garbanati, D., *Class field theory summarized*, Rocky Mountain Journal of Mathematics, Denver, 1981.
6. Gelabart, S., *An elementary introduction to the Langlands program*, Bulletin of the american mathematical society, Providence, 1984.
7. Janusz, G., *Algebraic number fields*, Academic press, 1973.
8. Koblitz, N., *p-adic numbers, p-adic analysis and zeta functions*, Springer, New York, 1984.
9. Ivorra Castillo, C., *Teoría de cuerpos de clase*, Disponible a www.uv.es/ivorra, Valencia.
10. Lemmermeyer, F., *Reciprocity laws: from Euler to Einsenstein*, Springer, Morikeweg, 2000.
11. Milne, J.S., *Algebraic number theory*, Disponible a www.jsmilne.org/math/, 2017.
12. Milne, J.S., *Class field theory*, Disponible a www.jsmilne.org/math/, 2013.
13. Serre, J.P., Paris, *A course in arithmetics*, Springer, 1979.
14. Serre, J.P., *Local fields*, Springer, Paris, 1979.
15. Sharifi, R., *Group and Galois cohomology*, Disponible a http://math.ucla.edu/ sharifi/, 2016.